



Security Feature Guide for the QFX Series

Release

14.1x53



Modified: 2016-11-14

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.

Security Feature Guide for the QFX Series
14.1x53
Copyright © 2016, Juniper Networks, Inc.
All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

	About the Documentation	xvii
	Documentation and Release Notes	xvii
	Supported Platforms	xvii
	Using the Examples in This Manual	xvii
	Merging a Full Example	xviii
	Merging a Snippet	xviii
	Documentation Conventions	xix
	Documentation Feedback	xxi
	Requesting Technical Support	xxi
	Self-Help Online Tools and Resources	xxi
	Opening a Case with JTAC	xxii
Part 1	Firewall Filters	
Chapter 1	Using Firewall Filters	3
	Overview of Firewall Filters	3
	Firewall Filter Types	4
	Firewall Filter Components	5
	Firewall Filter Processing	5
	Understanding Firewall Filters on OVSDb-Managed Interfaces	5
	Example: Applying a Firewall Filter to OVSDb-Managed Interfaces	6
	Understanding How Firewall Filters Are Evaluated	8
	Understanding How Firewall Filters Control Packet Flows	10
	Understanding Firewall Filter Match Conditions	11
	Filter Match Conditions	11
	Numeric Filter Match Conditions	12
	Interface Filter Match Conditions	12
	IP Address Filter Match Conditions	13
	MAC Address Filter Match Conditions	13
	Bit-Field Filter Match Conditions	14
	Firewall Filter Match Conditions and Actions	15
	Understanding How a Firewall Filter Tests a Protocol	32
	Understanding Firewall Filter Planning	32
	Planning the Number of Firewall Filters to Create	34
	Understanding How Many Firewall Filters Are Supported	34
	Egress Filters	35
	Avoid Configuring too Many Filters	35
	Configuring TCAM Error Messages	36
	Policers can Limit Egress Filters	36
	Planning for Filter-Specific Policers	37
	Planning for Filter-Based Forwarding	37

Understanding Firewall Filter Processing Points for Bridged and Routed	
Packets	38
Configuring Firewall Filters	39
Configuring a Firewall Filter	39
Applying a Firewall Filter to a Port	41
Applying a Firewall Filter to a VLAN	41
Applying a Firewall Filter to a Layer 3 (Routed) Interface	41
Applying Firewall Filters to Interfaces	42
Example: Configuring Storm Control to Prevent Network Outages	43
Configuring a Firewall Filter to De-Encapsulate GRE Traffic on a QFX5100 or	
OCX Switch	45
Configuring a Filter to De-Encapsulate GRE Traffic	45
Applying the Filter to an Interface	46
Configuring MPLS Firewall Filters and Policers	47
Configuring MPLS Firewall Filters	47
Examples: Configuring MPLS Firewall Filters	48
Configuring Policers for LSPs	48
LSP Policer Limitations	49
Monitoring Firewall Filter Traffic	49
Monitoring Traffic for All Firewall Filters and Policers That Are	
Configured	49
Monitoring Traffic for a Specific Firewall Filter	50
Monitoring Traffic for a Specific Policer	50
Verifying That Firewall Filters Are Operational	50
Troubleshooting Firewall Filter Configuration	51
Firewall Filter Configuration Returns a No Space Available in TCAM	
Message	52
Filter Counts Previously Dropped Packet	53
Matching Packets Not Counted	54
Counter Reset When Editing Filter	54
Cannot Include loss-priority and policer Actions in Same Term	54
Cannot Egress Filter Certain Traffic Originating on QFX Switch	55
Firewall Filter Match Condition Not Working with Q-in-Q Tunneling	55
Egress Firewall Filters with Private VLANs	55
Egress Filtering of L2PT Traffic Not Supported	56
Cannot Drop BGP Packets in Certain Circumstances	56
Invalid Statistics for Policer	57
Policers can Limit Egress Filters	57

Part 2

Chapter 2

Policers

Using Policers	61
Overview of Policers	61
Policer Overview	62
Policer Types	62
Policer Actions	63
Policer Colors	64
Filter-Specific Policers	64
Suggested Naming Convention for Policers	65

Policer Counters	65
Policer Algorithms	65
How Many Policers Are Supported?	65
Policers Can Limit Egress Firewall Filters	66
Understanding Policers with Link Aggregation Groups	67
Understanding Color-Blind Mode for Single-Rate Tricolor Marking	67
Understanding Color-Aware Mode for Single-Rate Tricolor Marking	68
Summary of PLP Changes	68
Effect on Green Packets (Low PLP)	68
Effect on Yellow Packets (Medium PLP)	69
Effect on Red Packets (High PLP)	69
Understanding Color-Blind Mode for Two-Rate Tricolor Marking	69
Understanding Color-Aware Mode for Two-Rate Tricolor Marking	70
Summary of PLP Changes	70
Effect on Green Packets (Low PLP)	70
Effect on Yellow Packets (Medium PLP)	71
Effect on Red Packets (High PLP)	71
Understanding Policers on OVSDB-Managed Interfaces	72
Example: Applying a Policer to OVSDB-Managed Interfaces	72
Example: Using Two-Color Policers and Prefix Lists	75
Example: Using Policers to Manage Oversubscription	78
Assigning Forwarding Classes and Loss Priority	80
Configuring Color-Blind Egress Policers for Medium-Low PLP	82
Configuring Two-Color and Three-Color Policers to Control Traffic Rates	82
Configuring Two-Color Policers	83
Configuring Three-Color Policers	83
Specifying Policers in a Firewall Filter Configuration	84
Applying a Firewall Filter That Includes a Policer	84
Verifying That Three-Color Policers Are Operational	84
Verifying That Two-Color Policers Are Operational	85
Troubleshooting Policer Configuration	85
Incomplete Count of Packet Drops	86
Counter Reset When Editing Filter	86
Invalid Statistics for Policer	86
Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured	86
Filter-Specific Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured	87
Policers Can Limit Egress Filters	88
 Part 3	
 Chapter 3	
Media Access Control Security (MACsec)	
Using MACsec	93
Understanding Media Access Control Security (MACsec)	93
How MACsec Works	94
Understanding Connectivity Associations and Secure Channels	94

Understanding MACsec Security Modes	95
Understanding Static Connectivity Association Key Security Mode (Recommended Security Mode for Switch-to-Switch Links)	95
Understanding Dynamic Secure Association Key Security Mode (Switch-to-Host Links)	95
Understanding Static Secure Association Key Security Mode (Supported for Switch-to-Switch Links)	96
Understanding the Requirements to Enable MACsec on a Switch-to-Host Link	97
Understanding MACsec Hardware Requirements for EX Series and QFX Series Switches	97
Understanding MACsec Software Requirements for EX Series and QFX Series Switches	98
Understanding the MACsec Feature License Requirement	99
MACsec Limitations	99
Configuring Media Access Control Security (MACsec)	99
Acquiring and Downloading the Junos OS Software	100
Acquiring and Downloading the MACsec Feature License	101
Configuring the PIC Mode of the MACsec-capable Interfaces (EX4200 switches only)	102
Configuring MACsec Using Static Connectivity Association Key Security Mode (Recommended for Enabling MACsec on Switch-to-Switch Links)	103
Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link	107
Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link	111

Part 4

Chapter 4

Using Port Security

Port Security	119
Overview of Access Port Protection	119
Mitigation of Ethernet Switching Table Overflow Attacks	119
Mitigation of Rogue DHCP Server Attacks	120
Protection Against ARP Spoofing Attacks	120
Protection Against DHCP Snooping Database Alteration Attacks	121
Protection Against DHCP Starvation Attacks	121
Understanding Port Security	122
Understanding DHCP Snooping for Port Security	124
DHCP Snooping Basics	124
DHCP Snooping Process	125
DHCPv6 Snooping	126
Rapid Commit for DHCPv6	126
DHCP Server Access	127
Switching Device, DHCP Clients, and DHCP Server Are All on the Same VLAN	127
Switching Device Acts as DHCP Server	128
Switching Device Acts as Relay Agent	129
Static IP Address Additions to the DHCP Snooping Database	130

Snooping DHCP Packets That Have Invalid IP Addresses	130
Prioritizing Snooped Packets	131
Verifying That DHCP Snooping Is Working Correctly	131
Understanding DAI for Port Security	132
Address Resolution Protocol	132
ARP Spoofing	133
Dynamic ARP Inspection	133
Prioritizing Inspected Packets	134
Verifying That DAI Is Working Correctly	135
Understanding MAC Limiting and MAC Move Limiting for Port Security	135
MAC Limiting	136
MAC Move Limiting	136
Actions for MAC Limiting	137
MAC Addresses That Exceed the MAC Limit or MAC Move Limit	137
Verifying That MAC Limiting Is Working Correctly	137
Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly	138
Verifying That Allowed MAC Addresses Are Working Correctly	138
Verifying That Interfaces Are Shut Down	139
Customizing the Ethernet Switching Table Display to View Information for a Specific Interface	140
Verifying That MAC Move Limiting Is Working Correctly	140
Verifying That the Port Error Disable Setting Is Working Correctly	141
Understanding Trusted and Untrusted Ports	142
Understanding Trusted DHCP Servers for Port Security	142
Verifying That a Trusted DHCP Server Is Working Correctly	143
Understanding DHCP Option 82 for Port Security	144
DHCP Option 82 Processing	144
Suboption Components of Option 82	145
Configurations That Support Option 82	145
Understanding Static ARP Entries	146

Part 5

Chapter 5

Using Device Security

Device Security	151
Understanding Storm Control	151
Understanding Unicast RPF	153
Unicast RPF for Switches Overview	153
Unicast RPF Implementation	154
Unicast RPF Packet Filtering	154
Bootstrap Protocol (BOOTP) and DHCP Requests	154
Default Route Handling	154
When to Enable Unicast RPF	154
When Not to Enable Unicast RPF	155
Limitations of the Unicast RPF Implementation on EX3200, EX4200, EX4300, and EX4500 Switches	156

	Understanding Unknown Unicast Forwarding	157
	Example: Configuring Storm Control to Prevent Network Outages	157
	Verifying That the Port Error Disable Setting Is Working Correctly	159
	Configuring Unicast RPF (CLI Procedure)	160
	Disabling Unicast RPF (CLI Procedure)	162
	Verifying Unicast RPF Status	162
	Configuring Unknown Unicast Forwarding (CLI Procedure)	165
Part 6	Using DDOS Protection	
Chapter 6	Overview of DDOS Protection	169
	Understanding Distributed Denial-of-Service Protection on QFX Series	
	Switches	169
	Policer Enforcement Points on QFX Series Switches	170
Chapter 7	Configuring DDOS Protection	171
	Example: Configuring DDoS Protection on QFX Series Switches	171
	Disabling DDoS Protection Policers and Logging Globally	174
	Configuring DDoS Protection Policers on QFX Series Switches	174
	Configuring the Aggregate Policer for a Protocol Group	175
	Configuring Policers' Bandwidth and Burst Values on the Switch	176
	Disabling Policers and Policer Logging	176
	Tracing DDoS Protection Operations	177
	Configuring the DDoS Protection Trace Log Filename	178
	Configuring the Number and Size of DDoS Protection Log Files	178
	Configuring Access to the DDoS Protection Log File	178
	Configuring a Regular Expression for DDoS Protection Messages to Be	
	Logged	179
	Configuring the DDoS Protection Tracing Flags	179
	Configuring the Severity Level to Filter Which DDoS Protection Messages	
	Are Logged	179
Chapter 8	Monitoring DDOS Protection	181
	Verifying and Managing DDoS Protection	181
Part 7	Configuration Statements and Operational Commands	
Chapter 9	Configuration Statements for Firewall Filters	185
	family	186
	filter	187
	filter (Layer 2 and Layer 3 Interfaces)	188
	filter (VLANs)	189
	firewall	190
	from	191
	interface-specific	192
	term	193
	then (Filters)	194
Chapter 10	Configuration Statements for Policers	195
	action	196
	bandwidth-limit	196

	burst-size-limit	197
	color-aware	198
	color-blind	199
	committed-burst-size	200
	committed-information-rate	201
	excess-burst-size	202
	filter-specific	203
	firewall	204
	if-exceeding	205
	loss-priority high then discard (Three-Color Policer)	206
	peak-burst-size	207
	peak-information-rate	208
	policer	209
	single-rate	210
	then (Policers)	211
	three-color-policer	212
	two-rate	213
Chapter 11	Configuration Statements for MACsec	215
	cak	216
	ckn	217
	connectivity-association	218
	connectivity-association (MACsec Interfaces)	219
	direction	220
	encryption	221
	exclude-protocol	222
	id	223
	include-sci	224
	interfaces (MACsec)	225
	key	226
	key-server-priority	227
	mac-address (MACsec)	228
	macsec	229
	mka	230
	must-secure	231
	no-encryption	232
	offset	233
	port-id	234
	pre-shared-key	235
	replay-protect	236
	replay-window-size	237
	secure-channel	238
	security-association	239
	security-mode	240
	transmit-interval (MACsec)	241
Chapter 12	Configuration Statements for Port Security	243
	circuit-id	244
	dhcp-snooping-file	245
	fc-map	246

	fcoe-trusted	248
	mac-move-limit	249
	no-allowed-mac-log	250
	no-gratuitous-arp-request	251
	persistent-learning	251
	port-error-disable	252
	vendor-id	254
	write-interval	255
Chapter 13	Configuration Statements for Device Security	257
	action-shutdown	258
	bandwidth-level	259
	bandwidth-percentage	260
	interface (Unknown Unicast Forwarding)	261
	no-broadcast	262
	no-multicast	263
	no-unknown-unicast	264
	rpf-check	265
	storm-control	266
	storm-control-profiles	267
	unknown-unicast-forwarding	268
Chapter 14	Configuration Statements for DDoS Protection	269
	bandwidth (DDoS)	270
	bandwidth-scale (DDoS)	271
	burst (DDoS)	272
	burst-scale (DDoS)	273
	ddos-protection (DDoS)	274
	disable-fpc (DDoS)	275
	disable-logging (DDoS)	276
	disable-routing-engine (DDoS)	277
	fpc (DDoS)	278
	global (DDoS)	279
	protocols (DDoS)	280
	recover-time (DDoS)	283
	traceoptions (DDoS)	284
Chapter 15	Firewall Operational Commands	287
	clear firewall	288
	show firewall	289
	show firewall policer	293
	show interfaces filters	295
	show pfe filter hw summary	297
Chapter 16	MACsec Operational Commands	299
	clear security mka statistics	300
	show security macsec connections	301
	show security macsec statistics	303
	show security mka sessions	307
	show security mka statistics	309

Chapter 17	Port Security Operational Commands	311
	clear arp inspection statistics	312
	clear dhcp snooping binding	313
	clear ethernet-switching port-error	314
	show dhcp snooping binding	315
Chapter 18	DDos Protection Operational Commands	317
	clear ddos-protection protocols	318
	show ddos-protection protocols	320
	show ddos-protection protocols parameters	336
	show ddos-protection protocols statistics	343
	show ddos-protection statistics	354
	show ddos-protection version	355

List of Figures

Part 1	Firewall Filters	
Chapter 1	Using Firewall Filters	3
	Figure 1: Evaluation of Terms Within a Firewall Filter	9
	Figure 2: Application of Firewall Filters to Control Packet Flow	11
Part 2	Policers	
Chapter 2	Using Policers	61
	Figure 3: Flow of Tricolor Marking Policer Operation	62
Part 4	Using Port Security	
Chapter 4	Port Security	119
	Figure 4: DHCP Server Connected Directly to a Switching Device	128
	Figure 5: DHCP Server Connected Directly to Switching Device 2, with Switching Device 2 Connected to Switching Device 1 Through a Trusted Trunk Port . . .	128
	Figure 6: Switching Device Is the DHCP Server	129
	Figure 7: Switching Device Acting as Relay Agent Through Router to DHCP Server	130
	Figure 8: Switch Relays DHCP Requests to Server	146
Part 5	Using Device Security	
Chapter 5	Device Security	151
	Figure 9: Symmetrically Routed Interfaces	155
	Figure 10: Asymmetrically Routed Interfaces	156

List of Tables

	About the Documentation	xvii
	Table 1: Notice Icons	xix
	Table 2: Text and Syntax Conventions	xix
Part 1	Firewall Filters	
Chapter 1	Using Firewall Filters	3
	Table 3: Actions for Firewall Filters	14
	Table 4: Supported Match Conditions for Firewall Filters	15
	Table 5: Actions for Firewall Filters	28
	Table 6: Action Modifiers for Firewall Filters	29
	Table 7: Supported Firewall Filter Numbers	34
Part 2	Policers	
Chapter 2	Using Policers	61
	Table 8: Policer Actions	63
	Table 9: Color-Blind Mode TCM Color-to-PLP Mapping	67
	Table 10: Color-Aware Mode Single-Rate PLP Mapping	68
	Table 11: Color-Blind Mode TCM Color-to-PLP Mapping	69
	Table 12: Color-Aware Mode Two-Rate PLP Mapping	70
	Table 13: Servers Connected to Switch	78
	Table 14: Unicast Forwarding Classes	80
Part 4	Using Port Security	
Chapter 4	Port Security	119
	Table 15: DHCPv6 Messages and Equivalent DHCPv4 Messages	126
Part 7	Configuration Statements and Operational Commands	
Chapter 14	Configuration Statements for DDoS Protection	269
	Table 16: Protocol Groups Supported by DDoS Protection on QFX Series Switches	281
Chapter 15	Firewall Operational Commands	287
	Table 17: show firewall Output Fields	289
	Table 18: show firewall policer Output Fields	293
	Table 19: show interfaces filters Output Fields	295
	Table 20: show pfe filter hw summary Output Fields	297
Chapter 16	MACsec Operational Commands	299

	Table 21: show security macsec connections Output Fields	301
	Table 22: show security macsec statistics Output Fields	303
	Table 23: show security mka sessions Output Fields	307
	Table 24: show security mka statistics Output Fields	309
Chapter 17	Port Security Operational Commands	311
	Table 25: show dhcp snooping binding Output Fields	315
Chapter 18	DDos Protection Operational Commands	317
	Table 26: show ddos-protection protocols Output Fields	327
	Table 27: show ddos-protection protocols parameters Output Fields	337
	Table 28: show ddos-protection protocols statistics Output Fields	344
	Table 29: show ddos-protection statistics Output Fields	354
	Table 30: show ddos-protection version Output Fields	355

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:

- [QFX Series standalone switches](#)

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 [CLI Explorer](#).

Documentation Conventions

[Table 1 on page xix](#) defines notice icons used in this guide.

Table 1: Notice Icons

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

[Table 2 on page xix](#) defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: 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.	user@host> show chassis alarms No alarms currently active
<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 of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

- 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

Firewall Filters

- [Using Firewall Filters on page 3](#)

CHAPTER 1

Using Firewall Filters

- [Overview of Firewall Filters on page 3](#)
- [Understanding Firewall Filters on OVSDb-Managed Interfaces on page 5](#)
- [Example: Applying a Firewall Filter to OVSDb-Managed Interfaces on page 6](#)
- [Understanding How Firewall Filters Are Evaluated on page 8](#)
- [Understanding How Firewall Filters Control Packet Flows on page 10](#)
- [Understanding Firewall Filter Match Conditions on page 11](#)
- [Firewall Filter Match Conditions and Actions on page 15](#)
- [Understanding How a Firewall Filter Tests a Protocol on page 32](#)
- [Understanding Firewall Filter Planning on page 32](#)
- [Planning the Number of Firewall Filters to Create on page 34](#)
- [Understanding Firewall Filter Processing Points for Bridged and Routed Packets on page 38](#)
- [Configuring Firewall Filters on page 39](#)
- [Applying Firewall Filters to Interfaces on page 42](#)
- [Example: Configuring Storm Control to Prevent Network Outages on page 43](#)
- [Configuring a Firewall Filter to De-Encapsulate GRE Traffic on a QFX5100 or OCX Switch on page 45](#)
- [Configuring MPLS Firewall Filters and Policers on page 47](#)
- [Monitoring Firewall Filter Traffic on page 49](#)
- [Verifying That Firewall Filters Are Operational on page 50](#)
- [Troubleshooting Firewall Filter Configuration on page 51](#)

Overview of Firewall Filters

Firewall filters provide rules that define whether to accept or discard packets that are transiting an interface. If a packet is accepted, you can configure additional actions to perform on the packet, such as class-of-service (CoS) marking (grouping similar types of traffic together and treating each type of traffic as a class with its own level of service priority) and traffic policing (controlling the maximum rate of traffic sent or received). You configure firewall filters to determine whether to accept or discard a packet before it enters or exits any of these:

- Port
- VLAN
- Layer 3 (routed) interface
- Routed VLAN interface (RVI)

An *ingress* firewall filter is applied to packets that are entering an interface or VLAN, and an *egress* firewall filter is applied to packets that are exiting an interface or VLAN.



NOTE: Firewall filters are sometimes called *access control lists (ACLs)*.

- [Firewall Filter Types on page 4](#)
- [Firewall Filter Components on page 5](#)
- [Firewall Filter Processing on page 5](#)

Firewall Filter Types

The following firewall filter types are supported:

- Port (Layer 2) firewall filter—Port firewall filters apply to Layer 2 traffic transiting system ports.
- VLAN firewall filter—VLAN firewall filters provide access control for packets that enter a VLAN, are bridged within a VLAN, or leave a VLAN.
- Router (Layer 3) firewall filter—You can apply a router firewall filter in both ingress and egress directions on IPv4 or IPv6 Layer 3 (routed) interfaces, routed VLAN interfaces (RVI) and a loopback interface, which filters traffic sent to the switch itself or generated by the switch. (You apply a filter to a loopback interface in the input direction to protect the switch from unwanted traffic. You also might want to apply a filter to a loopback interface in the output direction so that you can set the forwarding class and DSCP bit value for packets that originate on the switch itself. This feature gives you very fine control over the classification of CPU generated packets. For example, you might want to assign different DSCP values and forwarding classes to traffic generated by different routing protocols so the traffic for those protocols can be treated in a differentiated manner by other devices. You can apply a filter to a loopback interface in the output direction starting with Junos OS 13.2X51-D15.)



NOTE: You can apply a firewall filter to a management interface (for example, `me0`) on a QFX and EX4600 standalone switch. You cannot apply a firewall filter to a management interface on a QFX3000-G or QFX3000-M system.

- MPLS filter—You can apply a firewall filter to an MPLS interface

To apply a firewall filter:

1. Configure the firewall filter.

2. Apply the firewall filter to a port, VLAN, or router interface.



NOTE: You can apply only one firewall filter to a port, VLAN, or interface for a given direction. For example, for interface ge-0/0/6.0, you can apply one filter for the ingress direction and one for the egress direction.

Firewall Filter Components

In a firewall filter, you first define the family address type (ethernet-switching, inet (for IPv4), inet6 (for IPv6), or mpls) and then define one or more terms that specify the filtering criteria and the action to take if a match occurs.

Each term consists of the following components:

- Match conditions—Specify values that a packet must contain to be considered a match. You can specify values for most fields in the IP, TCP, UDP, or ICMP headers. You can also match on interface names.
- Action—Specifies what to do if a packet matches the match conditions. A filter can accept, discard, or reject a matching packet and then perform additional actions, such as counting, classifying, and policing. If no action is specified for a term, the default is to accept the matching packet.

Firewall Filter Processing

If there are multiple terms in a filter, the order of the terms is important. If a packet matches the first term, the switch executes the action defined by that term, and no other terms are evaluated. If the switch does not find a match between the packet and the first term, it compares the packet to the next term. If no match occurs between the packet and the second term, the system continues to compare the packet to each successive term in the filter until a match is found. If the packet does not match any terms in the filter, the switch discards the packet by default.

Related Documentation

- [Understanding Firewall Filter Planning on page 32](#)
- [Understanding Firewall Filter Processing Points for Bridged and Routed Packets on page 38](#)
- [Understanding How Firewall Filters Are Evaluated on page 8](#)
- [Understanding Firewall Filter Match Conditions on page 11](#)
- [Overview of Policers on page 61](#)
- [Configuring Firewall Filters on page 39](#)

Understanding Firewall Filters on OVSDb-Managed Interfaces

When you use a Contrail controller to manage VXLANs on a QFX switch (through the Open vSwitch Database—OVSDb—management protocol), the VXLAN interfaces are automatically configured with the **flexible-vlan-tagging** and **encapsulation**

extended-vlan-bridge statements. Starting with Junos OS Release 14.1X53-D30, you can create **family ethernet-switching** logical units (subinterfaces) on these interfaces. This enables you to apply Layer 2 (**family ethernet-switching**) firewall filters to these subinterfaces, which means that you apply firewall filters to OVSDB-managed interfaces. These filters support all the same match conditions and actions as any other Layer 2 filter.



WARNING: Firewall filters are the only supported configuration items on **family ethernet-switching** subinterfaces of OVSDB-managed interfaces. Layer 2 (port) filters are the only allowed filters.

Because a Contrail controller can create subinterfaces dynamically, you need to apply firewall filters in such a way that the filters will apply to subinterfaces whenever the controller creates them. You accomplish this by using configuration groups to configure and apply the firewall filters. See [“Example: Applying a Firewall Filter to OVSDB-Managed Interfaces” on page 6](#) for more information.

**Related
Documentation**

- [Example: Applying a Firewall Filter to OVSDB-Managed Interfaces on page 6](#)
- [Overview of Firewall Filters on page 3](#)
- [Understanding VXLANs](#)
- [Understanding the OVSDB Protocol Running on Juniper Networks Devices](#)
- [Understanding Policers on OVSDB-Managed Interfaces on page 72](#)

Example: Applying a Firewall Filter to OVSDB-Managed Interfaces

Starting with Junos OS Release 14.1X53-D30, you can create **family ethernet-switching** logical units (subinterfaces) on VXLAN interfaces managed by a Contrail controller. (The controller and switch communicate through the Open vSwitch Database—OVSDB—management protocol). This support enables you to apply Layer 2 (**family ethernet-switching**) firewall filters to these subinterfaces, which means that you apply firewall filters to OVSDB-managed interfaces. Because a Contrail controller can create subinterfaces dynamically, you need to apply firewall filters in such a way that the filters will apply to subinterfaces whenever the controller creates them. You accomplish this by using configuration groups to configure and apply the firewall filters. (You must use configuration groups for this purpose—that is, you cannot apply a firewall filter directly to these subinterfaces.)



NOTE: Firewall filters are the only supported configuration items on family **ethernet-switching** subinterfaces of OVSDB-managed interfaces. Layer 2 (port) filters are the only allowed filters.

- [Requirements on page 7](#)
- [Overview on page 7](#)
- [Configuration on page 7](#)

Requirements

This example uses the following hardware and software components:

- A QFX5100 switch
- Junos OS Release 14.1X53-D30 or later

Overview

This example assumes that interfaces xe-0/0/0 and xe-0/0/1 on the switch are VXLAN interfaces managed by a Contrail controller, which means that the controller has applied the **flexible-vlan-tagging** and **encapsulation extended-vlan-bridge** statements to these interfaces. You want to apply a firewall filter that accepts traffic from the Web to any subinterfaces that the controller creates dynamically. To apply a firewall filter Layer 2 (port) firewall filter to any dynamically created subinterfaces, you must create and apply the filter as shown in this example.

Configuration

To configure a firewall filter to be automatically applied to subinterfaces created dynamically by a Contrail controller, perform these tasks:

- [\[xref target has no title\]](#)

CLI Quick Configuration

```
[edit]
set groups vxlan-filter-group interfaces xe-0/0/0 unit <*> family ethernet-switching filter input vxlan-filter
set groups vxlan-filter-group interfaces xe-0/0/1 unit <*> family ethernet-switching filter input vxlan-filter
set groups vxlan-filter-group firewall family ethernet-switching filter vxlan-filter term t1 from destination-port 80
set groups vxlan-filter-group firewall family ethernet-switching filter vxlan-filter term t1 then accept
set apply-groups vxlan-filter-group
```

Step-by-Step Procedure

1. Create configuration group **vxlan-filter-group** to apply firewall filter **vxlan-filter** to any subinterface of interface xe-0/0/0. The filter applies to any subinterface because you specify **unit <*>**:


```
[edit]
user@switch# set groups vxlan-filter-group interfaces xe-0/0/0 unit <*> family ethernet-switching filter input vxlan-filter
```
2. Create the same configuration for interface xe-0/0/1:

[edit]

```
user@switch# set groups vxlan-filter-group interfaces xe-0/0/1 unit <*> family ethernet-switching filter input vxlan-filter
```

3. Configure the group to include a family **ethernet-switching** filter that matches on outgoing traffic to the web:

[edit]

```
user@switch# set groups vxlan-filter-group firewall family ethernet-switching filter vxlan-filter term t1 from destination-port 80
```

4. Configure the group to accept the traffic that matches the filter:

[edit]

```
user@switch# set groups vxlan-filter-group firewall family ethernet-switching filter vxlan-filter term t1 then accept
```

5. Apply the group to enable its configuration:

[edit]

```
user@switch# set apply-groups vxlan-filter-group
```

Related Documentation

- *Understanding Junos OS Configuration Groups*
- [Overview of Firewall Filters on page 3](#)
- *Understanding VXLANs*
- *Understanding the OVSDb Protocol Running on Juniper Networks Devices*
- [Example: Applying a Policer to OVSDb-Managed Interfaces on page 72](#)

Understanding How Firewall Filters Are Evaluated

A firewall filter consists of one or more terms, and the order of the terms within a filter is important. Before you configure firewall filters, you should understand how switches evaluate the terms within a filter and how packets are evaluated against the terms.

When a firewall filter consists of a single term, the filter is evaluated as follows:

- If the packet matches all the conditions, the action in the **then** statement is taken.
- If the packet matches all the conditions, and no action is specified in the **then** statement, the default action **accept** is taken.
- If the packet does not match all the conditions, the switch discards it.

When a firewall filter consists of more than one term, the filter is evaluated sequentially:

1. The packet is evaluated against the conditions in the **from** statement in the first term.
2. If the packet matches all the conditions in the term, the action in the **then** statement is taken and the evaluation ends. Subsequent terms in the filter are not evaluated.
3. If the packet does not match all the conditions in the term, the packet is evaluated against the conditions in the **from** statement in the second term.

This process continues until the packet matches all the conditions in the **from** statement in one of the subsequent terms or there are no more terms in the filter.

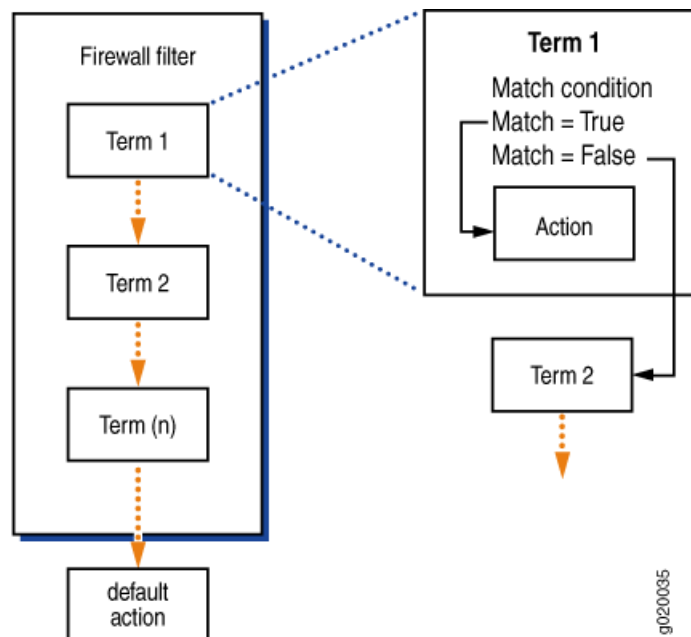
4. If a packet passes through all the terms in the filter without a match, the switch discards it.



NOTE: The order of conditions in a **from** statement is not important because a packet must match all the conditions to be considered a match.

Figure 1 on page 9 shows how switches evaluate the terms within a firewall filter.

Figure 1: Evaluation of Terms Within a Firewall Filter



If you do not include a **from** statement in a term, all packets will match the term and be processed by the **then** statement. If a term does not contain a **then** statement or if an action has not been configured in the **then** statement, the term accepts any matching packets.

Every firewall filter contains an implicit **deny** statement at the end of the filter, which is equivalent to the following explicit filter term:

```
term implicit-rule {
  then discard;
}
```

Consequently, a packet that does not match any of the terms in a firewall filter is discarded. If you configure a filter that has no terms, all packets that pass through the filter are discarded.



NOTE: Firewall filtering is supported on packets that are at least 64 bytes long.

**Related
Documentation**

- [Understanding Firewall Filter Match Conditions on page 11](#)
- [Overview of Policers on page 61](#)
- [Configuring Firewall Filters on page 39](#)

Understanding How Firewall Filters Control Packet Flows

A switch supports firewall filters that allow you to control flows of data packets and local packets. *Data packets* transit a switch as they are forwarded from a source to a destination. *Local packets* are destined for or sent by a Routing Engine (they do not transit a switch). Local packets usually contain routing protocol data, data for IP services such as Telnet or SSH, or data for administrative protocols such as the Internet Control Message Protocol (ICMP).

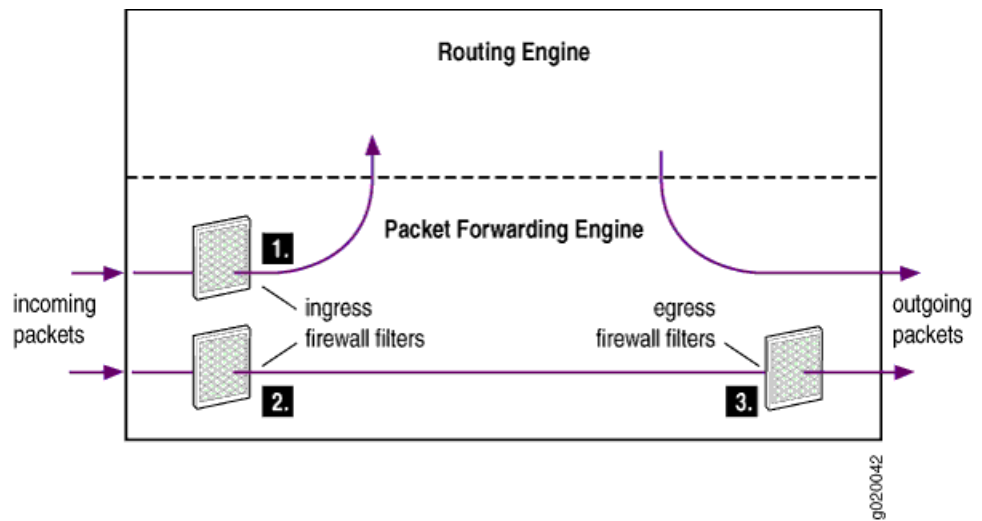
Firewall filters affect packet flows entering into or exiting from a switch as follows:

- Ingress firewall filters affect the flow of data packets that are received on switch interfaces. When a switch receives a data packet, the Packet Forwarding Engine in the system that contains the ingress interface determines where to forward the packet by looking in its Layer 2 or Layer 3 forwarding table for the best route to the destination. Data packets are forwarded to an egress interface. Locally destined packets are forwarded to the Routing Engine.
- Egress firewall filters affect data packets that are transiting a switch but do not affect packets sent by the Routing Engine. These filters are applied by the Packet Forwarding Engine in the system that contains the egress interface.

[Figure 2 on page 11](#) illustrates the application of ingress and egress firewall filters to control the flow of packets through a switch:

1. Ingress firewall filter applied to locally destined packets that are received on switch interfaces and are destined for the Routing Engine.
2. Ingress firewall filter applied to data packets that are received on switch interfaces and will transit the switch.
3. Egress firewall filter applied to data packets that are transiting the switch.

Figure 2: Application of Firewall Filters to Control Packet Flow



Related Documentation

- [Understanding Firewall Filter Processing Points for Bridged and Routed Packets on page 38](#)
- [Understanding How Firewall Filters Are Evaluated on page 8](#)
- [Configuring Firewall Filters on page 39](#)

Understanding Firewall Filter Match Conditions

Before you define terms for firewall filters, you must understand how the conditions in a term are handled and how to specify interface, numeric, address, and bit-field filter match conditions to achieve the desired filter results.

- [Filter Match Conditions on page 11](#)
- [Numeric Filter Match Conditions on page 12](#)
- [Interface Filter Match Conditions on page 12](#)
- [IP Address Filter Match Conditions on page 13](#)
- [MAC Address Filter Match Conditions on page 13](#)
- [Bit-Field Filter Match Conditions on page 14](#)

Filter Match Conditions

In the **from** statement of a firewall filter term, you specify the conditions that the packet must match for the action in the **then** statement to be taken. All conditions must match for the action to be implemented. The order in which you specify match conditions is not important, because a packet must match all the conditions in a term for a match to occur.

If you specify multiple values for the same condition, a match on any one of those values matches that condition. For example, if you specify multiple IP source addresses using the **source-address** statement, a packet that contains any one of those IP source addresses

matches the condition. In some cases you can specify multiple values for the same condition by enclosing the possible values in square brackets, as in:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set protocol (icmp | udp)
```

In other cases you must enter multiple statements, as in:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-address 10.1.1.1
user@switch# set source-address 10.1.1.2
```

If you specify no match conditions in a term, that term matches all packets.



NOTE: Unlike traditional Junos OS firewall filters, you cannot use **except** in a condition statement to negate the condition.

Numeric Filter Match Conditions

You can specify numeric filter match conditions that are identified by a numeric value, such as port and protocol numbers. For numeric filter match conditions, you specify the condition and a single value that a field in a packet must contain to be considered a match.

You can specify the numeric value in one of the following ways:

- Single number—A match occurs if the value of the field matches the number. For example, to match Telnet traffic:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-port 23
```

- Text synonym for a single number—A match occurs if the value of the field matches the number that corresponds to the synonym. For example, to match Telnet traffic:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-port telnet
```

- To specify multiple values for the same match condition in a filter term, enter each value in its own match statement. For example, a match occurs in the following term if the value of the source port in the packet is 22 or 23.

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-port 22
user@switch# set source-port 23
```

Interface Filter Match Conditions

You can specify an interface filter match condition to match an interface on which a packet is received or transmitted. For example, if you apply a filter to a VLAN you might want the filter to match on some interfaces that participate in the VLAN and not match on other interfaces in the VLAN. When you specify the name of the interface, you must include a logical unit.

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set interface ge-0/0/6.0
```

In this example, the final character (**O**) specifies the logical unit. You can include the wildcard (*****) as part of the interface name. For example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set interface ge-0/*/6.O
user@switch# set interface ge-0/1/*O
user@switch# set interface ge-0/0/6.*
```

Note that you must specify a value or a wildcard for the logical unit.

IP Address Filter Match Conditions

You can specify an address filter match condition to match an IP source or destination address or prefix in a packet. Specify the address or prefix type and the address or prefix itself. For example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-address 10.2.1.0/24;
```

If you omit the prefix length, it defaults to **/32**. For example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-address 10
[edit firewall family family-name filter filter-name term term-name from]
user@switch# show
destination-address {
  10.0.0.0/32;
}
```

To specify more than one IP address or prefix in a filter term, enter each address or prefix in its own match statement. For example, a match occurs in the following term if the source address of a packet matches either of the following prefixes:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-address 10.1.0.0/16
user@switch# set source-address 10.2.0.0/16
```

MAC Address Filter Match Conditions

You can specify a MAC address filter match condition to match a source or destination MAC address. You specify the address type and value that a packet must contain to be considered a match.

You can specify the MAC address as six hexadecimal bytes in any of the following formats:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-mac-address 00:11:22:33:44:55
```

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-mac-address 0011.2233.4455
```

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-mac-address 001122334455
```

Regardless of the formats you use, the system resolves the address to the standard format, in this case **00:11:22:33:44:55**.

To specify more than one MAC address in a filter term, enter each MAC address in its own match statement. For example, a match occurs in the following term if the value of the MAC source address matches either of the following addresses:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-mac-address 00:11:22:33:44:55
```

```
user@switch# set source-mac-address 00:11:22:33:20:15
```

Bit-Field Filter Match Conditions

You can specify bit-field filter match conditions to match particular bits within certain fields in Ethernet frames and IP, TCP, UDP, and ICMP headers. You usually specify the field and the bit within the field that must be set in a packet to be considered a match.

In most cases you can use a keyword to specify the bit you want to match on. For example, to match on a TCP SYN packet you can enter **syn**, as in:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags syn
```

You can also enter **0x02** because the SYN bit is the third least-significant bit of the 8-bit tcp-flags field:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags 0x02
```

To match multiple bit-field values, use the logical operators, which are described in [Table 3 on page 14](#). The operators are listed in order from highest precedence to lowest precedence. Operations are evaluated from left to right.

Table 3: Actions for Firewall Filters

Logical Operators	Description
!	Negation
&	Logical AND
	Logical OR

If you use a logical operator, enclose the values in quotation marks and do not include any spaces. For example, the following statement matches the second packet of a TCP handshake:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags "syn&ack"
```

To negate a match, precede the value with an exclamation point. For example, the following statement matches only the initial packet of a TCP handshake:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags "syn&!ack"
```

You can use text synonyms to specify some common bit-field matches. For example, the following statement also matches the initial packet of a TCP handshake:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-initial
```

Related Documentation

- [Understanding How a Firewall Filter Tests a Protocol on page 32](#)
- [Firewall Filter Match Conditions and Actions on page 15](#)
- [Configuring Firewall Filters on page 39](#)

Firewall Filter Match Conditions and Actions

Each term in a firewall filter consists of *match conditions* and an *action*. Match conditions are the fields and values that a packet must contain to be considered a match. You can define single or multiple match conditions in *match statements*. You can also include no match statement, in which case the term matches all packets.

When a packet matches a filter, a switch takes the action specified in the term. In addition, you can specify action modifiers to count, mirror, rate-limit, and classify packets. If no match conditions are specified for the term, the switch accepts the packet by default.

This topic describes the various match conditions, actions, and action modifiers that you can define in a firewall filter.

- [Table 4 on page 15](#) describes the match conditions you can specify when configuring a firewall filter. Some of the numeric range and bit-field match conditions allow you to specify a text synonym. To see a list of all the synonyms for a match condition, type ? at the appropriate place in a statement.
- [Table 5 on page 28](#) shows the actions that you can specify in a term.
- [Table 6 on page 29](#) shows the action modifiers you can use to count, mirror, rate-limit, and classify packets.



NOTE: On switches that do not support Layer 2 features (such as the OCX1100), you can use only those match conditions that are valid for IPv4 and IPv6 interfaces.

Table 4: Supported Match Conditions for Firewall Filters

Match Condition	Description	Direction and Interface
arp-type	ARP request packet or ARP reply packet.	Egress and ingress ports.
destination-address <i>ip-address</i>	IP destination address field, which is the address of the final destination node.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.
destination-mac-address <i>mac-address</i>	Destination media access control (MAC) address of the packet.	Ingress ports, VLANs and IPv4 (inet) interfaces. Egress ports and VLANs.

Table 4: Supported Match Conditions for Firewall Filters (*continued*)

Match Condition	Description	Direction and Interface
destination-port value	<p>TCP or UDP destination port field. Typically, you specify this match in conjunction with the protocol match statement. For the following well-known ports you can specify text synonyms (the port numbers are also listed):</p> <p>afs (1483), bgp (179), biff (512), bootpc (68), bootps (67),</p> <p>cmd (514), cvspserver (2401),</p> <p>dhcp (67), domain (53),</p> <p>eklogin (2105), ekshell (2106), exec (512),</p> <p>finger (79), ftp (21), ftp-data (20),</p> <p>http (80), https (443),</p> <p>ident (113), imap (143),</p> <p>kerberos-sec (88), klogin (543), kpasswd (761), krb-prop (754), krbupdate (760), kshell (544),</p> <p>ldap (389), login (513),</p> <p>mobileip-agent (434), mobileip-mn (435), msdp (639),</p> <p>netbios-dgm (138), netbios-ns (137), netbios-ssn (139), nfsd (2049), nntp (119), ntalk (518), ntp (123),</p> <p>pop3 (110), pptp (1723), printer (515),</p> <p>radacct (1813), radius (1812), rip (520), rkinit (2108),</p> <p>smtp (25), snmp (161), snmptrap (162), snpp (444), socks (1080), ssh (22), sunrpc (111), syslog (514),</p> <p>tacacs-ds (65), talk (517), telnet (23), tftp (69), timed (525),</p> <p>who (513),</p> <p>xmcp (177),</p> <p>zephyr-clt (2103), zephyr-hm (2104)</p>	<p>Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>
destination-port range-optimize range	<p>Match a range of TCP or UDP port ranges while using the available memory more efficiently. Using this condition allows you to configure more firewall filters than if you configure individual destination ports. (Not supported with filter-based forwarding.)</p>	<p>Egress and ingress IPv4 (inet) interfaces.</p>

Table 4: Supported Match Conditions for Firewall Filters (*continued*)

Match Condition	Description	Direction and Interface
destination-prefix-list <i>prefix-list</i>	IP destination prefix list field. You can define a list of IP address prefixes under a prefix-list alias for frequent use. Define this list at the [edit policy-options] hierarchy level. (Not supported with filter-based forwarding for IPv6 interfaces)	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces and IPv6 (inet6) interfaces.
dot1q-tag <i>number</i>	802.1Q VLAN ID field in the Ethernet frame. The tag values can be 1–4094.	Ingress ports and VLANs. Egress ports and VLANs (<i>Number</i> must be the VLAN ID of the VLAN you want to match).
dot1q-user-priority <i>number</i>	802.1Q priority field in the Ethernet frame (used for class-of-service priorities). Values can be 0–7. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): <ul style="list-style-type: none"> • best-effort (0)—Best effort • background (1)—Background • standard (2)—Standard or spare • excellent-load (3)—Excellent load • controlled-load (4)—Controlled load • video (5)—Video • voice (6)—Voice • network-control (7)—Network control reserved traffic 	Ingress ports and VLANs. Egress ports and VLANs.
dscp <i>value</i>	Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most-significant 6 bits of this byte form the DSCP. You can specify DSCP in hexadecimal, binary, or decimal form. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): <ul style="list-style-type: none"> • be—best effort (default) • ef (46)—as defined in RFC 3246, <i>An Expedited Forwarding PHB</i>. • af11 (10), af12 (12), af13 (14); af21 (18), af22 (20), af23 (22); af31 (26), af32 (28), af33 (30); af41 (34), af42 (36), af43 (38) These four classes, with three drop precedences in each class, for a total of 12 code points, are defined in RFC 2597, <i>Assured Forwarding PHB</i>. • cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, cs5 	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.

Table 4: Supported Match Conditions for Firewall Filters (*continued*)

Match Condition	Description	Direction and Interface
ether-type value	<p>Ethernet type field of a packet. The EtherType value specifies what protocol is being transported in the Ethernet frame. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed):</p> <ul style="list-style-type: none"> • aarp (0x80F3)—EtherType value AARP • appletalk (0x809B)—EtherType value AppleTalk • arp (0x0806)—EtherType value ARP • fcoe (0x8906)—EtherType value FCoE • fip (0x8914)—EtherType value FIP • ipv4 (0x0800)—EtherType value IPv4 • ipv6 (0x08DD)—EtherType value IPv6 • mpls-multicast (0x8848)—EtherType value MPLS multicast • mpls-unicast (0x8847)—EtherType value MPLS unicast • oam (0x88A8)—EtherType value OAM • ppp (0x880B)—EtherType value PPP • pppoe-discovery (0x8863)—EtherType value PPPoE Discovery Stage • pppoe-session (0x8864)—EtherType value PPPoE Session Stage • sna (0x80D5)—EtherType value SNA 	<p>Ingress ports and VLANs.</p> <p>Egress ports and VLANs.</p>
exp	Match on MPLS EXP bits.	<p>Ingress MPLS interfaces.</p> <p>Egress MPLS interfaces.</p>
fragment-flags value	<p>IP fragmentation flags. In place of the numeric value, you can specify one of the following text synonyms (the hexadecimal values are also listed):</p> <ul style="list-style-type: none"> • is-fragment • dont-fragment (0x4000) • more-fragments (0x2000) • reserved (0x8000) 	Ingress ports and VLANs.

Table 4: Supported Match Conditions for Firewall Filters (*continued*)

Match Condition	Description	Direction and Interface
from-fabric	<p>(QFabric systems only) Traffic flows forwarded from a QFabric system Interconnect device egress interface to a Node device ingress interface.</p> <p>In one “from” filter term, use one or more of the following match conditions to identify a flow of traffic:</p> <ul style="list-style-type: none"> Client-side MAC address (for example, an FCF MAC address for FCoE traffic) (destination-mac-address <i>mac-address</i>) or source-mac-address <i>mac-address</i>) Server-side MAC address (for example, an ENode MAC address for FCoE traffic) (destination-mac-address <i>mac-address</i>) or source-mac-address <i>mac-address</i>) EtherType (ether-type <i>value</i>) <p>NOTE: If you remap an FCoE flow using EtherType as the match condition, you need to include two terms in the filter in each direction of flow to identify the traffic, one term to identify FCoE traffic (EtherType 0x8906), and one term to identify FIP traffic (EtherType 0x8914).</p> <ul style="list-style-type: none"> VLAN (vlan (<i>vlan-name</i> <i>vlan-id</i>)) .1q user priority (dot1q-user-priority) <p>In the same “from” filter term, use the “from-fabric” match condition to match traffic flowing from the Interconnect device to the Node device. In the “then” statement of the filter term, remap the identified traffic flow from the forwarding class used on the Interconnect device back into its original forwarding class, by specifying the original forwarding class and loss priority as action modifiers. This programs the QFabric system to use the original forwarding class for the flow when the flow is forwarded out of the QFabric system, not the temporarily remapped forwarding class the flow uses as it crosses the Interconnect device. The “to-fabric” match condition, which you configure using a different term in the same filter, maps the flow from the original forwarding class into a new forwarding class at the Node device egress, before the traffic crosses the Interconnect device. The “to-fabric” and the “from-fabric” match conditions combine to enable you to avoid traffic flow fate sharing as the traffic crosses the Interconnect device. The to-fabric match condition allows you to separate the flow into multiple forwarding classes as it crosses the Interconnect device, and the from-fabric match condition brings the traffic back together into the same forwarding class before the traffic leaves the QFabric system.</p>	VLANs. Filter applies to traffic forwarded from an Interconnect device to a Node device.

Table 4: Supported Match Conditions for Firewall Filters (*continued*)

Match Condition	Description	Direction and Interface
icmp-code value	<p>ICMP code field. Because the meaning of the value depends upon the associated icmp-type, you must specify a value for icmp-type along with a value for icmp-code. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed). The keywords are grouped by the ICMP type with which they are associated:</p> <ul style="list-style-type: none"> <i>IPv4</i>: parameter-problem—ip-header-bad (0), required-option-missing (1) <i>IPv6</i>: parameter-problem—ip6-header-bad (0), unrecognized-next-header (1), unrecognized-option (2) redirect—redirect-for-network (0), redirect-for-host (1), redirect-for-tos-and-net (2), redirect-for-tos-and-host (3) time-exceeded—ttl-eq-zero-during-reassembly (1), ttl-eq-zero-during-transit (0) <i>IPv4</i>: unreachable—network-unreachable (0), host-unreachable (1), protocol-unreachable (2), port-unreachable (3), fragmentation-needed (4), source-route-failed (5), destination-network-unknown (6), destination-host-unknown (7), source-host-isolated (8), destination-network-prohibited (9), destination-host-prohibited (10), network-unreachable-for-TOS (11), host-unreachable-for-TOS (12), communication-prohibited-by-filtering (13), host-precedence-violation (14), precedence-cutoff-in-effect (15) <i>IPv6</i>: unreachable—address-unreachable (3), administratively-prohibited (1), no-route-to-destination (0), port-unreachable (4) 	<p>Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>
hop-limitvalue	Match the the specified hop limit or set of hop limits. Specify a single value or a range of values from 0 through 255.	Ingress and egress IPv6 (inet6) interfaces.

Table 4: Supported Match Conditions for Firewall Filters (*continued*)

Match Condition	Description	Direction and Interface
icmp-type <i>value</i>	<p>ICMP message type field. Typically, you specify this match in conjunction with the protocol match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed):</p> <p><i>IPv4</i>: echo-reply (0), destination unreachable (3), source-quench (4), redirect (5), echo-request (8), IPv4 (inet)-advertisement (9), IPv4 (inet)-solicit (10), time-exceeded (11), parameter-problem (12), timestamp (13), timestamp-reply (14), info-request (15), info-reply (16), mask-request (17), mask-reply (18)</p> <p><i>IPv6</i>: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), membership-query (130), membership-report (131), membership-termination (132), router-solicit (133), router-advertisement (134), neighbor-solicit (135), neighbor-advertisement (136), redirect (137), router-renumbering (138), node-information-request (139), node-information-reply (140)</p> <p>See also icmp-code <i>variable</i>.</p>	<p>Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>
interface <i>interface-name</i>	<p>Interface on which the packet is received, including the logical unit. You can include the wildcard character (*) as part of an interface name or logical unit.</p> <p>NOTE: An interface from which a packet is sent cannot be used as a match condition.</p>	<p>Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p> <p>Egress IPv4 (inet) interfaces and IPv6 (inet6) interfaces.</p>
ip-destination-address <i>address</i>	IPv4 address that is the final destination node address for the packet.	Ingress ports and VLANs.
ip6-destination-address <i>address</i>	IPv6 address that is the final destination node address for the packet.	Ingress ports and VLANs. (You cannot simultaneously apply a filter with this match criterion to a Layer 2 port and VLAN that includes that port.)
ip-options	Specify any to create a match if anything is specified in the options field in the IP header.	<p>Ingress ports, VLANs, and IPv4 (inet) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>
ip-precedence <i>ip-precedence-field</i>	<p>IP precedence field. In place of the numeric field value, you can specify one of the following text synonyms (the field values are also listed): critical-ecp (0xa0), flash (0x60), flash-override (0x80), immediate (0x40), internet-control (0xc0), net-control (0xe0), priority (0x20), or routine (0x00).</p>	<p>Ingress ports, VLANs, and IPv4 (inet) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>

Table 4: Supported Match Conditions for Firewall Filters (*continued*)

Match Condition	Description	Direction and Interface
ip-protocol <i>number</i>	IP protocol field.	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
ip-source-address <i>address</i>	IPv4 address of the source node sending the packet.	Ingress ports and VLANs.
ip6-source-address <i>address</i>	IPv6 address of the source node sending the packet.	Ingress ports and VLANs. (You cannot simultaneously apply a filter with this match criterion to a Layer 2 port and VLAN that includes that port.)
ip-version <i>address</i>	IP version of the packet. Use this condition to match IPv4 or IPv6 header fields in traffic that arrives on a Layer 2 port or VLAN interface.	Ingress ports and VLANs.
is-fragment	Using this condition causes a match if the More Fragments flag is enabled in the IP header or if the fragment offset is not zero.	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
l2-encap-type <i>llc-non-snap</i>	Match on logical link control (LLC) layer packets for non-Subnet Access Protocol (SNAP) Ethernet Encapsulation type.	Ingress ports and VLANs. Egress ports and VLANs.
label	Match on MPLS label bits.	Ingress MPLS interfaces. Egress MPLS interfaces.
learn-vlan-id <i>number</i>	Matches the ID of a normal VLAN or the ID of the outer (service) VLAN (for Q-in-Q VLANs). The acceptable values are 1-4095.	Ingress ports and VLANs. Egress ports and VLANs.
next-header	IPv4 or IPv6 protocol value. In place of the numeric value, you can specify one of the following text synonyms (the numeric values are also listed): hop-by-hop (0), icmp (1), icmp6 (58), igmp (2), ipip (4), tcp (6), egp (8), udp (17), ipv6 (41), routing (43), fragment (44), rsvp (46), gre (47), esp (50), ah (51), icmp6 (58), no-next-header (59), dstopts (60), ospf (89), pim (103), vrrp (112), sctp (132)	Ingress ports, VLANs, and IPv6 (inet6) interfaces. Egress IPv6 (inet6) interfaces.
packet-length	Packet length in bytes. You must enter a value between 0 and 65535.	Ingress ports, VLANs, IPv4 (inet), and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.

Table 4: Supported Match Conditions for Firewall Filters (*continued*)

Match Condition	Description	Direction and Interface
payload-protocol	<p>IPv4 or IPv6 protocol value. In place of the numeric value, you can specify one of the following text synonyms (the numeric values are also listed):</p> <p>hop-by-hop (0), icmp (1), icmp6 (58), igmp (2), ipip (4), tcp (6), egp (8), udp (17), ipv6 (41), routing (43), fragment (44), rsvp (46), gre (47), esp (50), ah (51), icmp6 (58), no-next-header (59), dstopts (60), ospf (89), pim (103), vrrp (112), sctp (132)</p>	<p>Ingress ports, VLANs, and IPv6 (inet6) interfaces.</p> <p>Egress IPv6 (inet6) interfaces.</p>
precedence value	<p>IP precedence bits in the type-of-service (ToS) byte in the IP header. (This byte can also be used for the DiffServ DSCP.) In place of the numeric value, you can specify one of the following text synonyms (the numeric values are also listed):</p> <ul style="list-style-type: none"> • routine (0) • priority (1) • immediate (2) • flash (3) • flash-override (4) • critical-ecp (5) • internet-control (6) • net-control (7) 	<p>Ingress ports, VLANs, and IPv4 (inet) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>
protocol type	<p>IPv4 or IPv6 protocol value. In place of the numeric value, you can specify one of the following text synonyms (the numeric values are also listed):</p> <p>hop-by-hop (0), icmp (1), icmp6, igmp (2), ipip (4), tcp (6), egp (8), udp (17), ipv6 (41), routing (43), fragment (44), rsvp (46), gre (47), esp (50), ah (51), icmp6 (58), no-next-header (59), dstopts (60), ospf (89), pim (103), vrrp (112), sctp (132)</p>	<p>Ingress ports, VLANs and IPv4 (inet) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>

Table 4: Supported Match Conditions for Firewall Filters (*continued*)

Match Condition	Description	Direction and Interface
rat-type tech-type-value	<p>Match the radio-access technology (RAT) type specified in the 8-bit Tech-Type field of Proxy Mobile IPv4 (PMIPv4) access technology type extension. The technology type specifies the access technology through which the mobile device is connected to the access network. Specify a single value, a range of values, or a set of values. You can specify a technology type as a numeric value from 0 through 255 or as a system keyword.</p> <ul style="list-style-type: none"> Numeric value 1 matches IEEE 802.3. Numeric value 2 matches IEEE 802.11a/b/g. Numeric value 3 matches IEEE 802.16e. Numeric value 4 matches IEEE 802.16m. Text string eutran matches 4G. Text string geran matches 2G. Text string utran matches 3G. . 	Egress and ingress IPv4 (inet) interfaces.
sample	Sample the packet traffic. Apply this option only if you have enabled traffic sampling.	Egress and ingress IPv4 (inet) interfaces.
source-address ip-address	IP source address field, which is the address of the node that sent the packet.	<p>Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>
source-mac-address mac-address	Source media access control (MAC) address of the packet.	<p>Ingress ports and VLANs.</p> <p>Egress ports and VLANs.</p>
source-port value	TCP or UDP source port. Typically, you specify this match in conjunction with the protocol match statement. In place of the numeric field, you can specify one of the text synonyms listed under destination-port .	<p>Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>
source-port range-optimize range	Match a range of TCP or UDP port ranges while using the available memory more efficiently. Using this condition allows you to configure more firewall filters than if you configure individual source ports. (Not supported with filter-based forwarding.)	Egress and ingress IPv4 (inet) interfaces.
source-prefix-list prefix-list	IP source prefix list. You can define a list of IP address prefixes under a prefix-list alias for frequent use. Define this list at the [edit policy-options] hierarchy level. (Not supported with filter-based forwarding for IPv6 interfaces)	<p>Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>

Table 4: Supported Match Conditions for Firewall Filters (*continued*)

Match Condition	Description	Direction and Interface
tcp-established	<p>Match packets of an established TCP connection. This condition matches packets other than those used to set up a TCP connection—that is, three-way handshake packets are not matched.</p> <p>When you specify tcp-established, a switch does not implicitly verify that the protocol is TCP. You must also specify the protocol tcp match condition.</p>	<p>Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>
tcp-flags value	<p>One or more TCP flags:</p> <ul style="list-style-type: none"> • ack (0x10) • fin (0x01) • push (0x08) • rst (0x04) • syn (0x02) • urgent (0x20) 	<p>Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>
tcp-initial	<p>Match the first TCP packet of a connection. A match occurs when the TCP flag SYN is set and the TCP flag ACK is not set.</p> <p>When you specify tcp-initial, a switch does not implicitly verify that the protocol is TCP. You must also specify the protocol tcp match condition.</p>	<p>Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>

Table 4: Supported Match Conditions for Firewall Filters (*continued*)

Match Condition	Description	Direction and Interface
to-fabric <except>		VLANs. Filter applies to traffic forwarded from a Node device to the Interconnect device.

Table 4: Supported Match Conditions for Firewall Filters (*continued*)

Match Condition	Description	Direction and Interface
	<p>(QFabric systems only) Traffic flows forwarded from a QFabric system Node device egress interface to an Interconnect device ingress interface.</p> <p>In one “from” filter term, use one or more of the following match conditions to identify a flow of traffic:</p> <ul style="list-style-type: none"> Client-side MAC address (for example, an FCF MAC address for FCoE traffic) (destination-mac-address <i>mac-address</i>) or source-mac-address <i>mac-address</i>) Server-side MAC address (for example, an ENode MAC address for FCoE traffic) (destination-mac-address <i>mac-address</i>) or source-mac-address <i>mac-address</i>) EtherType (ether-type <i>value</i>) <p>NOTE: If you remap an FCoE flow using EtherType as the match condition, you need to include two terms in the filter in each direction of flow to identify the traffic, one term to identify FCoE traffic (EtherType 0x8906), and one term to identify FIP traffic (EtherType 0x8914).</p> <ul style="list-style-type: none"> VLAN (vlan (<i>vlan-name</i> <i>vlan-id</i>)) .1q user priority (dot1q-user-priority) <p>In the same “from” filter term, use the “to-fabric” match condition to match traffic flowing from the Node device to the Interconnect device. In the “then” statement of the filter term, remap the identified traffic flow from its current forwarding class into another forwarding class (default or user-defined) and loss priority by specifying the forwarding class and loss priority as action modifiers.</p> <p>The QFabric system uses the remapped forwarding class to transport the flow across the Interconnect device. The “from-fabric” match condition, which you configure using a different term in the same filter, maps the flow back to the original forwarding class after the flow traverses the Interconnect device, when the flow enters the Node device from which the traffic will egress from the QFabric system. The “to-fabric” and the “from-fabric” match conditions combine to enable you to avoid traffic flow fate sharing as the traffic crosses the Interconnect device. The to-fabric match condition allows you to separate the flow into multiple forwarding classes as it crosses the Interconnect device, and the from-fabric match condition brings the traffic back together into the same forwarding class before the traffic leaves the QFabric system.</p> <p>The except option matches traffic that is locally</p>	

Table 4: Supported Match Conditions for Firewall Filters (*continued*)

Match Condition	Description	Direction and Interface
	switched—that is, traffic that enters and exits the same QFabric system Node device and does not cross the Interconnect device. If traffic identified by the match conditions contains some flows that are locally switched, the “except” option remaps the forwarding class for the locally switched traffic and does <i>not</i> remap the forwarding class for remotely switched traffic.	
traffic-class	<p>8-bit field that specifies the class-of-service (CoS) priority of the packet. The traffic-class field is used to specify a DiffServ code point (DSCP) value. This field was previously used as the type-of-service (ToS) field in IPv4, and, the semantics of this field (for example, DSCP) are identical to those of IPv4.</p> <p>You can specify one of the following text synonyms (the field values are also listed):</p> <p>af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs0 (0), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56), ef (46)</p>	<p>Ingress ports, VLANs, and IPv6 (inet6) interfaces.</p> <p>Egress IPv6 (inet6) interfaces.</p>
ttl value	IP Time-to-live (TTL) field in decimal. The value can be 1-255.	<p>Ingress IPv4 (inet) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>
user-vlan-1p-priority value	Match on the IEEE 802.1p priority bits in the inner (customer) VLAN tag in a Q-in-Q VLAN. Specify a single value or multiple values from 0-7.	<p>Ingress ports, VLANs, and IPv4 (inet) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>
user-vlan-id number	Matches the ID of the inner (customer) VLAN in a Q-in-Q VLAN. The acceptable values are 1-4095.	<p>Ingress ports, VLANs, and IPv4 (inet) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>

Use **then** statements to define actions that should occur if a packet matches all conditions in a **from** statement. [Table 5 on page 28](#) shows the actions that you can specify in a term. (If you do not include a **then** statement, the system accepts packets that match the filter.)

Table 5: Actions for Firewall Filters

Action	Description
accept	Accept a packet. This is the default action for packets that match a term.
discard	Discard a packet silently without sending an Internet Control Message Protocol (ICMP) message.

Table 5: Actions for Firewall Filters (*continued*)

Action	Description
reject <i>message-type</i>	<p>Discard a packet and send a “destination unreachable” ICMPv4 message (type 3). To log rejected packets, configure the syslog action modifier.</p> <p>You can specify one of the following message types: administratively-prohibited (default), bad-host-tos, bad-network-tos, host-prohibited, host-unknown, host-unreachable, network-prohibited, network-unknown, network-unreachable, port-unreachable, precedence-cutoff, precedence-violation, protocol-unreachable, source-host-isolated, source-route-failed, or tcp-reset.</p> <p>If you specify tcp-reset, the system sends a TCP reset if the packet is a TCP packet; otherwise nothing is sent.</p> <p>If you do not specify a message type, the ICMP notification “destination unreachable” is sent with the default message “communication administratively filtered.”</p> <p>NOTE: The reject action is supported on ingress interfaces only.</p>
routing-instance <i>instance-name</i>	Forward matched packets to a virtual routing instance.
vlan <i>VLAN-name</i>	<p>Forward matched packets to a specific VLAN.</p> <p>NOTE: The vlan action is supported on ingress interfaces only.</p> <p>NOTE: This action is not supported on OCX series switches.</p>

You can also specify the action modifiers listed in [Table 6 on page 29](#) to count, mirror, rate-limit, and classify packets.

Table 6: Action Modifiers for Firewall Filters

Action Modifier	Description
analyzer <i>analyzer-name</i>	<p>(Non-ELS platforms) Mirror traffic (copy packets) to an analyzer configured at the [edit ethernet-switching-options analyzer] hierarchy level.</p> <p>You can specify port mirroring for ingress port, VLAN, and IPv4 (inet) firewall filters only.</p>
count <i>counter-name</i>	Count the number of packets that match the term.
decapsulate [<i>gre</i> <i>routing-instance</i>]	De-encapsulate GRE packets or forward de-encapsulated GRE packets to the specified routing instance

Table 6: Action Modifiers for Firewall Filters (*continued*)

Action Modifier	Description
dscp value	<p>Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most-significant 6 bits of this byte form the DSCP.</p> <p>You can specify DSCP in hexadecimal, binary, or decimal form.</p> <p>In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed):</p> <ul style="list-style-type: none"> • be—best effort (default) • ef (46)—as defined in RFC 3246, <i>An Expedited Forwarding PHB</i>. • af11 (10), af12 (12), af13 (14); af21 (18), af22 (20), af23 (22); af31 (26), af32 (28), af33 (30); af41 (34), af42 (36), af43 (38) <p>These four classes, with three drop precedences in each class, for a total of 12 code points, are defined in RFC 2597, <i>Assured Forwarding PHB</i>.</p> <ul style="list-style-type: none"> • cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, cs5
forwarding-class class	<p>Classify the packet in one of the following default forwarding classes, or in a user-defined forwarding class:</p> <ul style="list-style-type: none"> • best-effort • fcoe • mcast • network-control • no-loss <p>NOTE: To configure a forwarding class, you must also configure loss priority.</p>
interface	<p>Switch the traffic to the specified interface without performing a lookup on it. This action is valid only when the filter is applied on ingress.</p>
log	<p>Log the packet's header information in the Routing Engine. To view this information, enter the show firewall log operational mode command.</p> <p>NOTE: The log action modifier is supported on ingress interfaces only.</p>
loss-priority (low medium-low medium-high high)	<p>Set the packet loss priority (PLP).</p> <p>NOTE: The medium-low option is not supported on QFX5100 switches.</p> <p>NOTE: The loss-priority action modifier is supported on ingress interfaces only.</p> <p>NOTE: The loss-priority action modifier is not supported in combination with the policer action.</p>

Table 6: Action Modifiers for Firewall Filters (*continued*)

Action Modifier	Description
policer <i>policer-name</i>	<p>Send packets to a policer (for the purpose of applying rate limiting).</p> <p>You can specify a policer for ingress port, VLAN, IPv4 (inet), IPv6 (inet6), and MPLS filters.</p> <p>NOTE: The policer action modifier is not supported in combination with the loss-priority action.</p>
port-mirror	<p>(ELS platforms) Mirror traffic (copy packets) to an output interface configured in a port-mirroring instance at the [edit forwarding-options port-mirroring] hierarchy level.</p> <p>You can specify port mirroring for ingress port, VLAN, and IPv4 (inet) firewall filters only.</p>
port-mirror-instance <i>port-mirror-instance-name</i>	<p>(ELS platforms) Mirror traffic to a port-mirroring instance configured at the [edit forwarding-options port-mirroring] hierarchy level.</p> <p>You can specify port mirroring for ingress port, VLAN, and IPv4 (inet) firewall filters only.</p> <p>NOTE: This action modifier is not supported on OCX series switches.</p>
syslog	<p>Log an alert for this packet.</p> <p>NOTE: The syslog action modifier is supported on ingress interfaces only.</p>
three-color-policer <i>three-color-policer-name</i>	<p>Send packets to a three-color policer (for the purpose of applying rate limiting).</p> <p>You can specify a three-color policer for ingress and egress port, VLAN, IPv4 (inet), IPv6 (inet6), and MPLS filters.</p> <p>NOTE: The policer action modifier is not supported in combination with the loss-priority action.</p>

- Related Documentation**
- [Understanding How Firewall Filters Are Evaluated on page 8](#)
 - [Understanding How a Firewall Filter Tests a Protocol on page 32](#)
 - [Overview of Policers on page 61](#)
 - [Understanding Port Mirroring](#)
 - [Configuring Firewall Filters on page 39](#)

Understanding How a Firewall Filter Tests a Protocol

When examining match conditions in a firewall filter, a switch tests only the fields that you specify. It does not implicitly test any fields that you do not explicitly configure. For example, if you specify a match condition of **source-port ssh**, there is no implied test to determine if the protocol is TCP. In this case, the switch considers any packet that has a value of **22** (decimal) in the 2-byte field that follows a *presumed* IP header to be a match. To ensure that the term matches on TCP packets, you also specify an **ip-protocol tcp** match condition.

For the following match conditions, you should explicitly specify the protocol match condition in the same term:

- **destination-port**—Specify protocol **tcp** or protocol **udp**.
- **icmp-code**—Specify protocol **icmp** and **icmp-type**.
- **icmp-type**—Specify protocol **icmp** or protocol **icmp6**.
- **source-port**—Specify protocol **tcp** or protocol **udp**.
- **tcp-flags**—Specify protocol **tcp**.

Related Documentation

- [Understanding Firewall Filter Match Conditions on page 11](#)
- [Configuring Firewall Filters on page 39](#)

Understanding Firewall Filter Planning

Before you create a firewall filter and apply it, determine what you want the filter to accomplish and how to use its match conditions and actions to achieve your goals. It is important that you understand how packets are matched, the default and configured actions of the firewall filter, and where to apply the firewall filter.

You can apply no more than one firewall filter per port, VLAN, or router interface per direction (input and output). For example, for a given port you can apply at most one filter in the input direction and one filter in the output direction. You should try to be conservative in the number of terms (rules) that you include in each firewall filter, because a large number of terms requires longer processing time during a commit operation and can make testing and troubleshooting more difficult.

Before you configure and apply firewall filters, answer the following questions for each of them:

1. What is the purpose of the filter?

For example, the system can drop packets based on header information, rate-limit traffic, classify packets into forwarding classes, log and count packets, or prevent denial-of-service attacks.

2. What are the appropriate match conditions? Determine the packet header fields that the packet must contain for a match. Possible fields include:

- Layer 2 header fields—Source and destination MAC addresses, 802.1Q tag, Ethernet type, or VLAN.
 - Layer 3 header fields—Source and destination IP addresses, protocols, and IP options (IP precedence, IP fragmentation flags, or TTL type).
 - TCP header fields—Source and destination ports and flags.
 - ICMP header fields—Packet type and code.
3. What are the appropriate actions to take if a match occurs?
- The system can accept, discard, or reject packets.
4. What additional action modifiers might be required?
- For example, you can configure the system to mirror (copy) packets to a specified port, count matching packets, apply traffic management, or police packets.
5. On what port, router interface, or VLAN should the firewall filter be applied?

Start with the following basic guidelines:

- If packets entering or leaving a Layer 2 interface (port) need to be filtered, apply the filter at the **[edit family ethernet switching filter]** hierarchy level. This is a port filter.
- If packets entering or leaving any port in a specific VLAN need to be filtered, use a VLAN filter.
- If packets entering or leaving a Layer 3 (routed) interface or routed VLAN interface (RVI) need to be filtered, use a router firewall filter. Apply the filter to the interface at the **[edit family inet]** hierarchy level. You can also apply a router firewall filter on a loopback interface.

Before you choose the interface or VLAN on which to apply a firewall filter, understand how that placement can affect traffic flow to other interfaces. In general, apply a filter close to the source device if the filter matches on source or destination IP addresses, IP protocols, or protocol information—such as ICMP message types, and TCP or UDP port numbers. However, you should apply a filter close to the destination device if the filter matches *only* on a source IP address. When you apply a filter too close to the source device, the filter could prevent that source device from accessing other services that are available on the network.



NOTE: Egress firewall filters do not affect the flow of locally generated control packets from the Routing Engine.

6. In which direction should the firewall filter be applied?

You typically configure different actions for traffic entering an interface than you configure for traffic exiting an interface.

7. How many filters should I create?

See [“Planning the Number of Firewall Filters to Create” on page 34](#) for information about how many firewall filters you can apply.

- Related Documentation**
- [Overview of Policers on page 61](#)
 - [Understanding How Firewall Filters Are Evaluated on page 8](#)
 - [Configuring Firewall Filters on page 39](#)

Planning the Number of Firewall Filters to Create

- [Understanding How Many Firewall Filters Are Supported on page 34](#)
- [Egress Filters on page 35](#)
- [Avoid Configuring too Many Filters on page 35](#)
- [Configuring TCAM Error Messages on page 36](#)
- [Policers can Limit Egress Filters on page 36](#)
- [Planning for Filter-Specific Policers on page 37](#)
- [Planning for Filter-Based Forwarding on page 37](#)

Understanding How Many Firewall Filters Are Supported

QFX3500, QFX3600, QFX5100, and EX4600 switches, QFabric Node devices, and VCF members support the maximum numbers of firewall filter terms per type of attachment point shown in [Table 7 on page 34](#).

Table 7: Supported Firewall Filter Numbers

Filter Type	QFX3500, QFX3600	QFX5100, EX4600
Ingress	768	1536
Egress	1024	1024

These totals are applied in aggregate. For example, on the QFX3500 and QFX3600 you can apply a total of 768 terms in all your port filters, Layer 3 filters, and VLAN filters that are applied in the input direction and 1024 terms in port filters, Layer 3 filters, and VLAN filters that are applied in the output direction.



NOTE: If you want to create more than 512 egress VLAN filters, your first VLAN ID should be 6 and the subsequent VLAN IDs should increase by 1. For example, to create 1024 egress VLAN filters, the first VLAN ID would be 6, the second ID would be 7, and the sequence would continue through VLAN ID 1029. Similarly, if you want to create fewer than 512 egress VLAN filters but want the total number of terms in those filters to exceed 512, you should number your VLAN IDs in the same manner. If you do not use this approach to create your VLAN IDs, the total number of allowed terms or filters will be less than 1024 and might be 512.

The ternary content addressable memory (TCAM) for firewall filters is divided into slices that accommodate 256 terms, and all the terms in a memory slice must be in filters of

the same type and applied in the same direction. A memory slice is reserved as soon as you commit a filter. For example, if you create a port filter and apply it in the input direction, a memory slice is reserved that will only store ingress port filters. If you create and apply only one ingress port filter and that filter has only one term, the rest of this slice is unused and is unavailable for other filter types.

Continuing with the above example for QFX3500 and QFX3600 switches, assume that you create and apply 256 ingress port filters with one term each so that one memory slice is filled. This leaves two more memory slices available for ingress filters. (Remember that the maximum number of ingress terms is 768.) If you then create and apply an ingress Layer 3 filter with one term, another memory slice is reserved for ingress Layer 3 filters. As before, the rest of the slice is unused and is unavailable for different filter types. At this point there is one memory slice available for any ingress filter type.

Now assume that you create and apply a VLAN ingress filter. The final memory slice is reserved for VLAN ingress filters. Memory allocation for ingress filters (once again assuming one term per filter) is as follows:

- Slice 1: Filled with 256 ingress port filters. You cannot commit any more ingress port filters.
- Slice 2: Contains one ingress Layer 3 filter with one term. You can commit 255 more terms in ingress Layer 3 filters.
- Slice 3: Contains one ingress VLAN filter with one term. You can commit 255 more terms in ingress VLAN filters.

Here is another example for QFX3500 and QFX3600 switches. Assume that you create 257 ingress port filters with one term per filter—that is, you create one more term than a single memory slice can accommodate. When you apply the filters and commit the configuration, the filter memory allocation is:

- Slice 1: Filled with 256 ingress port filters. You cannot apply any more ingress port filters.
- Slice 2: Contains one ingress port filter. You can apply 255 more terms in ingress port filters.
- Slice 3: This slice is unassigned. You can create and apply 256 terms in ingress filters of any type (port, Layer 3, or VLAN), but all the filters must be of the same type.

Egress Filters

All of the preceding principles also apply to egress filters, but four memory slices are used because IPv4 Layer 3 filters and IPv6 Layer 3 filters are stored in separate slices. The memory slices for egress filters are the same size as those for ingress filters, so the maximum number of egress filter terms is therefore 1024.

Avoid Configuring too Many Filters

If you violate any of these restrictions and commit a configuration that is not in compliance, Junos OS rejects the excessive filters. For example, if you configure 300 ingress port filters and 300 ingress Layer 3 filters and try to commit the configuration, Junos OS does the following (again assuming one term per filter):

- Accepts the 300 ingress port filters (storing them in two memory slices).
- Accepts the first 256 ingress Layer 3 filters it processes (storing them in the third memory slice).
- Rejects the remaining 44 ingress Layer 3 filters.



NOTE: In this situation, be sure to delete excessive filters (for example, the remaining 44 ingress Layer 3 filters) from the configuration before you reboot the device. If you reboot a device that has a noncompliant configuration, you cannot predict which filters are installed after the reboot. Using the example above, the 44 ingress Layer 3 filters that were originally rejected might be installed, and 44 of the port filters that were originally accepted might be rejected.

Configuring TCAM Error Messages

You can configure your switch to display error messages if a filter cannot be installed because there isn't enough TCAM space available. To have TCAM error messages sent to a syslog file, enter

```
set system syslog file filename pfe emergency
```

To have TCAM error messages sent to the console, enter

```
set system syslog console pfe emergency
```

To have TCAM error messages sent to an SSH terminal session, enter

```
set system syslog user user-login pfe emergency
```

Policers can Limit Egress Filters

The number of egress policers that you configure can affect the total number of allowed egress firewall filters. Every policer has two implicit counters that consume two entries in a 1024-entry TCAM that is used for counters, including counters that are configured as action modifiers in firewall filter terms. (Policers consume two entries because one is used for green packets and one is used for nongreen packets regardless of policer type.) If the TCAM becomes full, you cannot commit any more egress firewall filters that have terms with counters. For example, if you configure and commit 512 egress policers (two-color, three-color, or a combination of both policer types), all of the memory entries for counters are used up. If later in your configuration file you insert additional egress firewall filters with terms that also include counters, *none* of the terms in those filters are committed because there is no available memory space for the counters.

Here are some additional examples:

- Assume that you configure egress filters that include a total of 512 policers and no counters. Later in your configuration file you include another egress filter with 10 terms, 1 of which has a counter action modifier. None of the terms in this filter are committed because there is not enough TCAM space for the counter.

- Assume that you configure egress filters that include a total of 500 policers, so 1000 TCAM entries are occupied. Later in your configuration file you include the following two egress filters:
 - Filter A with 20 terms and 20 counters. All the terms in this filter are committed because there is enough TCAM space for all the counters.
 - Filter B comes after Filter A and has five terms and five counters. *None* of the terms in this filter are committed because there is not enough memory space for *all* the counters. (Five TCAM entries are required but only four are available.)

You can prevent this problem from occurring by ensuring that egress firewall filter terms with counter actions are placed earlier in your configuration file than terms that include policers. In this circumstance, Junos OS commits policers even if there is not enough TCAM space for the implicit counters. For example, assume the following:

- You have 1024 egress firewall filter terms with counter actions.
- Later in your configuration file you have an egress filter with 10 terms. None of the terms have counters but one has a policer action modifier.

You can successfully commit the filter with 10 terms even though there is not enough TCAM space for the implicit counters of the policer. The policer is committed without the counters.

Planning for Filter-Specific Policers

You can configure policers to be filter-specific, which means that Junos OS creates only one policer instance regardless of how many times the policer is referenced. When you do this, rate limiting is applied in aggregate, so if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, the total bandwidth allowed by the filter is 1 Gbps. However, the behavior of a filter-specific policer is affected by how the firewall filter terms that reference the policer are stored in ternary content addressable memory (TCAM). If you create a filter-specific policer and reference it in multiple firewall filter terms, the policer allows more traffic than expected if the terms are stored in different TCAM slices. For example, if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms that are stored in three separate memory slices, the total bandwidth allowed by the filter is 3 Gbps, not 1 Gbps.

To prevent this unexpected behavior from occurring, use the information about TCAM slices presented above to organize your configuration file so that all the firewall filter terms that reference a given filter-specific policer are stored in the same TCAM slice.

Planning for Filter-Based Forwarding

You can use firewall filters in conjunction with virtual routing instances to specify different routes for packets to travel in their networks. To set up this feature—called filter-based forwarding—you specify a filter and match criteria and then specify the virtual routing instance to send packets to. Filters used in this way also consume memory in an additional TCAM. See *Understanding FIP Snooping, FBF, and MVR Filter Scalability* for more

information. The section *FBF Filter VFP TCAM Consumption* in this topic specifically addresses the number of supported filters when using filter-based forwarding.



WARNING: Filter-based forwarding does not work with IPv6 interfaces on some Juniper switches.

**Related
Documentation**

- [Understanding How Firewall Filters Are Evaluated on page 8](#)
- [Understanding Firewall Filter Planning on page 32](#)
- [Configuring Firewall Filters on page 39](#)
- [Understanding Filter-Based Forwarding](#)

Understanding Firewall Filter Processing Points for Bridged and Routed Packets

You apply firewall filters at multiple processing points in the forwarding path. At each processing point, the action to be taken on a packet is determined by the configuration of the filter and the results of the lookup in the forwarding or routing table.

For both bridged (Layer 2) unicast packets and routed (Layer 3) unicast packets, firewall filters are applied in the prescribed order shown below (assuming that each filter is present and a packet is accepted by each one).

Bridged packets:

1. Ingress port filter
2. Ingress VLAN filter
3. Egress VLAN filter
4. Egress port filter

Routed packets:

1. Ingress port firewall filter
2. Ingress VLAN firewall filter (Layer 2 CoS)
3. Ingress router firewall filter (Layer 3 CoS)
4. Egress router firewall filter
5. Egress VLAN firewall filter
6. Egress port filter



NOTE: MAC learning occurs before filters are applied, so switches learn the MAC addresses of packets that are dropped by ingress filters.

- Related Documentation**
- [Overview of Firewall Filters on page 3](#)
 - [Understanding How Firewall Filters Control Packet Flows on page 10](#)
 - [Configuring Firewall Filters on page 39](#)

Configuring Firewall Filters

You can configure firewall filters in a switch to control traffic that enters switch ports or enters and exits VLANs and Layer 3 (routed) interfaces. To use a firewall filter, you must configure the filter and then apply it to a port, VLAN, or Layer 3 interface.

- [Configuring a Firewall Filter on page 39](#)
- [Applying a Firewall Filter to a Port on page 41](#)
- [Applying a Firewall Filter to a VLAN on page 41](#)
- [Applying a Firewall Filter to a Layer 3 \(Routed\) Interface on page 41](#)

Configuring a Firewall Filter

To configure a firewall filter:

1. Configure the family address type, filter name, term name, and at least one match condition—for example, match on packets that contain a specific source address:

```
[edit]
user@switch# set firewall family ethernet-switching filter ingress-port-filter term term-one
from source-address 192.0.2.14
```

For a firewall filter that is applied to a port or VLAN, specify the family address type **ethernet-switching**. For a firewall filter that is applied to a Layer 3 (routed) interface, specify the family address type **inet**.

The filter and term names can contain letters, numbers, and hyphens (-) and can be up to 64 characters long. Each filter name must be unique. A filter can contain one or more terms, and each term name must be unique within a filter.

2. Configure additional match conditions. For example, match on packets that contain a specific source port:

```
[edit firewall family ethernet-switching filter ingress-port-filter term
term-one from]
user@switch# set source-port 80
```

You can specify one or more match conditions in a single **from** statement. For a match to occur, the packet must match all the conditions in the term. The **from** statement is optional, but if included in a term, it cannot be empty. If you omit the **from** statement, all packets are considered to match.

3. If you want to apply a firewall filter to multiple interfaces and be able to see counters specific to each interface, configure the **interface-specific** option:

```
[edit firewall family ethernet-switching filter ingress-port-filter]
user@switch# set interface-specific
```

4. In each firewall filter term, specify the actions to take if the packet matches all the conditions in that term. You can specify an action and action modifiers:

- To specify a filter action, for example, to discard packets that match the conditions of the filter term:

```
[edit firewall family ethernet-switching filter ingress-port-filter term
term-one then]
user@switch# set discard
```

You can specify no more than one action (**accept**, **discard**, **reject**, **routing-instance**, or **vlan**) per term.

- To specify action modifiers, for example, to count and classify packets to a forwarding class:

```
[edit firewall family ethernet-switching filter ingress-port-filter term
term-one then]
user@switch# set count counter-one
user@switch# set forwarding-class expedited-forwarding
user@switch# set loss-priority high
```

You can specify any of the following action modifiers in a **then** statement:

- **analyzer *analyzer-name***—Mirror port traffic to a specified analyzer, which you must configure at the **[ethernet-switching-options]** level.
- **count *counter-name***—Count the number of packets that pass this filter term.



NOTE: We recommend that you configure a counter for each term in a firewall filter, so that you can monitor the number of packets that match the conditions specified in each filter term.



NOTE: On QFX3500 and QFX3600 switches, filters automatically count packets that have been dropped on ingress because of cyclic redundancy check (CRC) errors.

- **forwarding-class *class***—Assign packets to a forwarding class.
- **log**—Log the packet header information in the Routing Engine.
- **loss-priority *priority***—Set the priority of dropping a packet.
- **policer *policer-name***—Apply rate-limiting to the traffic.
- **syslog**—Log an alert for this packet.

If you omit the **then** statement or do not specify an action, packets that match all the conditions in the **from** statement are accepted. However, you should always explicitly configure an action in the **then** statement. You can include no more than one action statement, but you can use any combination of action modifiers. For an action or action modifier to take effect, all conditions in the **from** statement must match.



NOTE: Implicit discard is also applicable to a firewall filter applied to the loopback interface, lo0.

Applying a Firewall Filter to a Port

To apply a firewall filter to an ingress port:

1. Provide a meaningful description of the firewall filter in the configuration of the port to which the filter will be applied:

```
[edit]
user@switch# set interfaces ge-0/0/6 description "filter to limit tcp traffic at trunk port for employee-vlan"
```

2. Apply the filter to the interface, specifying the unit number, family address type, the direction of the filter (for packets entering the port), and the filter name:

```
[edit]
user@switch# set ge-0/0/6 unit 0 family ethernet-switching filter input ingress-port-filter
```

For firewall filters that are applied to ports, the family address type must be **ethernet-switching**.



NOTE: You can apply only one filter to a port for a given direction (ingress or egress).

Applying a Firewall Filter to a VLAN

To apply a firewall filter to a VLAN:

1. Provide a meaningful description of the firewall filter in the configuration of the VLAN to which the filter will be applied:

```
[edit]
user@switch# set vlans employee-vlan vlan-id 20 description "filter to block rogue devices on employee-vlan"
```

2. Apply firewall filters to filter packets that are entering or exiting the VLAN:

- To apply a filter to match packets that are entering the VLAN:

```
[edit]
user@switch# set vlans employee-vlan vlan-id 20 filter input ingress-vlan-rogue-block
```

- To apply a firewall filter to match packets that are exiting the VLAN:

```
[edit]
user@switch# set vlans employee-vlan vlan-id 20 filter output egress-vlan-filter
```



NOTE: You can apply only one filter to a VLAN for a given direction (ingress or egress).

Applying a Firewall Filter to a Layer 3 (Routed) Interface

To apply a firewall filter to a Layer 3 routed interface:

1. Provide a meaningful description of the firewall filter in the configuration of the interface to which the filter will be applied:

```
[edit]
```

```
user@switch# set interfaces ge-0/1/6 description "filter to count and monitor traffic on layer 3 interface"
```

2. You can apply firewall filters to filter packets that enter or exit a Layer 3 routed interface:

- To apply a firewall filter to filter packets that enter a Layer 3 interface:

```
[edit]
```

```
user@switch# set interfaces ge-0/1/6 unit 0 family inet filter input ingress-router-filter
```

- To apply a firewall filter to filter packets that exit a Layer 3 interface:

```
[edit]
```

```
user@switch# set interfaces ge-0/1/6 unit 0 family inet filter output egress-router-filter
```

For firewall filters applied to Layer 3 routed interfaces, the family address type must be **inet**.



NOTE: You can apply only one filter to an interface for a given direction (ingress or egress).

Related Documentation

- [Overview of Firewall Filters on page 3](#)
- [Firewall Filter Match Conditions and Actions on page 15](#)
- [Verifying That Firewall Filters Are Operational on page 50](#)
- [Monitoring Firewall Filter Traffic on page 49](#)
- [Configuring Port Mirroring](#)

Applying Firewall Filters to Interfaces

For a firewall filter to work, you must apply it to at least one interface. To do this, include the **filter** statement when configuring a logical interface at the **[edit interfaces]** hierarchy level:

```
[edit interfaces]
```

```
user@switch# set interface-name unit logical-unit-number family family-name filter (input | output) filter-name
```

In the **input** statement, specify a firewall filter to be evaluated when packets are received on the interface. Input filters applied to a loopback interface affect only traffic destined for the Routing Engine.

In the **output** statement, specify a filter to be evaluated when packets exit the interface.



NOTE: When you create a loopback interface, it is important to apply an ingress filter to it so the Routing Engine is protected. We recommend that when you apply a filter to the loopback interface lo0, you include the `apply-groups` statement. Doing so ensures that the filter is automatically inherited on every loopback interface, including lo0 and other loopback interfaces.

Related Documentation

- [Configuring Firewall Filters on page 39](#)

Example: Configuring Storm Control to Prevent Network Outages

Storm control enables you to prevent network outages caused by broadcast storms on the LAN. You can configure storm control on to rate-limit broadcast traffic, multicast traffic, and unknown unicast traffic at a specified level and to have packets dropped when the specified traffic level is exceeded, thereby preventing packets from proliferating and degrading the LAN.



NOTE: This example uses a Junos OS release that supports the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Example: Configuring Storm Control to Prevent Network Outages*.

- [Requirements on page 43](#)
- [Overview and Topology on page 43](#)
- [Configuration on page 44](#)

Requirements

This example uses the following hardware and software components:

- One QFX Series switch running Junos OS with ELS
- Junos OS Release 13.2 or later

Overview and Topology

A storm is generated when messages are broadcast on a network and each message prompts a receiving node to respond by broadcasting its own messages on the network. This, in turn, prompts further responses, creating a snowball effect and resulting in a broadcast storm that can cause network outages.

You can use storm control to prevent broadcast storms by specifying the amount, also known as the *storm control level*, of broadcast traffic, multicast traffic, and unknown unicast traffic to be allowed on an interface. You specify the storm control level as the traffic rate in kilobits per second (Kbps) of the combined applicable traffic streams or as the percentage of available bandwidth used by the combined applicable traffic streams.

On ELS systems, storm control is enabled by default on all interfaces at a level of 80 percent of the available bandwidth.

Storm control monitors the level of applicable incoming traffic and compares it with the level that you specify. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. As an alternative to having the switch drop packets, you can configure storm control to shut down interfaces or temporarily disable interfaces (see the **action-shutdown** statement or the **recovery-timeout** statement) when the storm control level is exceeded.



NOTE: If you configure storm control on an aggregated Ethernet interface, the storm-control level is applied to each member interface individually. For example, if the aggregated interface has two members and you configure a storm-control level of 20 kbps, Junos will not detect a storm if one or both of the member interfaces receives traffic at 15 kbps because in neither of these cases does an individual member receive traffic at a rate greater than the configured storm-control level. In this example, Junos detects a storm only if at least one member interface receives traffic at greater than 20 Kbps.

The topology used in this example consists of one switch connected to various network devices. This example shows how to configure the storm control level on interface xe-0/0/0 by setting the level to a traffic rate of 15,000 Kbps, based on the traffic rate of the combined applicable traffic streams. If the combined traffic exceeds this level, the switch drops packets for the controlled traffic types to prevent a network outage.

Configuration

CLI Quick Configuration

To quickly configure storm control based on the traffic rate in kilobits per second of the combined traffic streams, copy the following command and paste it into the switch terminal window:

```
[edit]
set forwarding-options storm-control-profiles sc-profile all bandwidth-level 15000
set interfaces xe-0/0/0 unit 0 family ethernet-switching storm-control sc-profile
```

Step-by-Step Procedure

To configure storm control:

1. Configure a storm control profile, **sc-profile**, and specify the traffic rate in kilobits per second of the combined traffic streams:

```
[edit]
user@switch> set forwarding-options storm-control-profiles sc-profile all bandwidth-level 15000
```

2. Bind the storm control profile, **sc**, to a logical interface:

```
[edit]
user@switch> set interfaces xe-0/0/0 unit 0 family ethernet-switching storm-control sc-profile
```

Results

Display the results of the configuration:

```
[edit forwarding-options]
user@switch> show storm-control-profiles sc-profile
```

```

all {
    bandwidth 15000;
}

[edit]
user@switch> show interfaces xe-0/0/0
unit 0 {
    family ethernet-switching {
        vlan {
            members default;
        }
        storm-control sc-profile;
    }
}

```

- Related Documentation**
- [Understanding Storm Control on page 151](#)
 - [Configuring Autorecovery for MAC Limited or Storm Control Interfaces \(CLI Procedure\)](#)

Configuring a Firewall Filter to De-Encapsulate GRE Traffic on a QFX5100 or OCX Switch

Generic routing encapsulation (GRE) provides a private, secure path for transporting packets through a network by encapsulating (or tunneling) the packets. GRE tunneling is performed by tunnel endpoints that encapsulate or de-encapsulate traffic.

You can use a firewall filter to de-encapsulate GRE traffic on a QFX5100 or OCX switch. This feature provides significant benefits in terms of scalability, performance, and flexibility because you don't need to create a tunnel interface to perform the de-encapsulation. For example, you can terminate many tunnels from multiple source IP addresses with one firewall term.



NOTE: QFX5100 and OCX switches support as many as 512 GRE tunnels, including tunnels created with a firewall filter. That is, you can create a total of 512 GRE tunnels, regardless of which method you use.

This topic describes:

1. [Configuring a Filter to De-Encapsulate GRE Traffic on page 45](#)
2. [Applying the Filter to an Interface on page 46](#)

Configuring a Filter to De-Encapsulate GRE Traffic

To configure a firewall filter to de-encapsulate GRE traffic:

1. Create an IPv4 firewall filter and (optionally) specify a source address for the tunnel:

```

[edit]
user@switch# set firewall family inet filter filter-name term term-name from
source-address address

```

You must create an IPv4 filter by using **family inet** because the outer header of a GRE packet must be IPv4. If you specify a source address, it should be an address on a device that will encapsulate traffic into GRE packets.



NOTE: To terminate many tunnels from multiple source IP addresses with one firewall term, do not configure a source address. In this case, the filter will de-encapsulate any GRE packets received by the interface that you apply the filter to.

2. Specify a destination address for the tunnel:

```
[edit ]
user@switch# set firewall family inet filter filter-name term term-name from
destination-address address
```

This should be an address on an interface of the switch on which you want the tunnel or tunnels to terminate and the GRE packets to be de-encapsulated. You should also configure this address as a tunnel endpoint on all the tunnel source routers that you want to form tunnels with the switch.

3. Specify that the filter should match and accept GRE traffic:

```
[edit ]
user@switch# set firewall family inet filter filter-name term term-name from protocol
gre
```

4. Specify that the filter should de-encapsulate GRE traffic:

```
[edit ]
user@switch# set firewall family inet filter filter-name term term-name then decapsulate
gre
```

Based on the configuration you have performed so far, the switch forwards the de-encapsulated packets by comparing the inner header to the default routing table (**inet0**). If you want the switch to use a virtual routing instance to forward the de-encapsulated packets, perform the following steps:

5. Specify the name of the virtual routing instance:

```
[edit ]
user@switch# set firewall family inet filter filter-name term term-name then decapsulate
routing-instance instance-name
```

6. Specify that the virtual routing instance is a virtual router:

```
[edit ]
user@switch# set routing-instances instance-name instance-type virtual-router
```

7. Specify the interfaces that belong to the virtual router:

```
[edit ]
user@switch# set routing-instances instance-name interface interface-name
```

Applying the Filter to an Interface

After you create the firewall filter, you must also apply it to an interface that will receive GRE traffic. Be sure to apply it in the input direction. For example, enter

```
[edit ]
user@switch# set interfaces interface-name unit logical-unit-number family inet filter
input filter-name
```

Because the outer header of a GRE packet must be IPv4, you must apply the filter to an IPv4 interface and specify **family inet**.

**Related
Documentation**

- [Understanding Generic Routing Encapsulation](#)
- [Configuring Generic Routing Encapsulation Tunneling](#)
- [Configuring Firewall Filters on page 39](#)

Configuring MPLS Firewall Filters and Policers

You can configure an MPLS firewall filter to count packets based on the EXP bits for the top-level MPLS label in a packet. You can also configure policers for MPLS LSPs.

The following sections discuss MPLS firewall filters and policers:

- [Configuring MPLS Firewall Filters on page 47](#)
- [Examples: Configuring MPLS Firewall Filters on page 48](#)
- [Configuring Policers for LSPs on page 48](#)

Configuring MPLS Firewall Filters

You can configure an MPLS firewall filter to count packets based on the EXP bits for the top-level MPLS label in a packet. You can then apply this filter to a specific interface on input or output. You can also configure a policer for the MPLS filter to police (that is, rate-limit) the traffic on the interface to which the filter is attached. You cannot apply MPLS firewall filters to loopback interfaces.

You can configure the following match conditions for MPLS filters at the **[edit firewall family mpls filter *filter-name* term *term-name* from]** hierarchy level:

- **exp**
- **label**

These **exp** match condition can accept EXP bits in the range 0 through 7. You can configure the following choices:

- A single EXP bit—for example, **exp 3**;
- Several EXP bits—for example, **exp 0, 4**;
- A range of EXP bits—for example, **exp [0-5]**;

The **label** match condition can accept a range of values from 0 to 1048575.

If you do not specify a match criterion (that is, you do not configure the **from** statement and use only the **then** statement with the **count** action keyword), all the MPLS packets passing through the interface on which the filter is applied will be counted.

You also can configure any of the following action keywords at the **[edit firewall family mpls filter *filter-name* term *term-name* then]** hierarchy level:

- **accept**
- **count**
- **discard**
- **policer**
- **three-color-policer**

Examples: Configuring MPLS Firewall Filters

The following examples illustrate how you might configure an MPLS firewall filter and then apply the filter to an interface. This filter is configured to count MPLS packets with EXP bits set to either 0 or 4.

The following shows a configuration for an MPLS firewall filter:

```
[edit firewall]
family mpls {
  filter expf {
    term expt0 {
      from {
        exp 0,4;
      }
      then {
        count counter0;
        accept;
      }
    }
  }
}
```

Configuring Policers for LSPs

MPLS LSP policing allows you to control the amount of traffic forwarded through a particular LSP. Policing helps to ensure that the amount of traffic forwarded through an LSP never exceeds the requested bandwidth allocation. LSP policing is supported on regular LSPs, LSPs configured with DiffServ-aware traffic engineering, and multiclass LSPs. You can configure multiple policers for each multiclass LSP. For regular LSPs, each LSP policer is applied to all of the traffic traversing the LSP. The policer's bandwidth limitations become effective as soon as the total sum of traffic traversing the LSP exceeds the configured limit.

You configure the multiclass LSP and DiffServ-aware traffic engineering LSP policers in a filter. The filter can be configured to distinguish between the different class types and apply the relevant policer to each class type. The policers distinguish between class types based on the EXP bits.

You configure LSP policers under the **family any** filter. The **family any** filter is used because the policer is applied to traffic entering the LSP. This traffic might be from different

families: IPv6, MPLS, and so on. You do not need to know what sort of traffic is entering the LSP, as long as the match conditions apply to all types of traffic.

LSP Policer Limitations

When configuring MPLS LSP policers, be aware of the following limitations:

- LSP policers are supported for packet LSPs only.
- LSP policers are supported for unicast next hops only. Multicast next hops are not supported.
- LSP policers are not supported on aggregated interfaces.
- The LSP policer runs before any output filters.
- Traffic sourced from the Routing Engine (for example, ping traffic) does not take the same forwarding path as transit traffic. This type of traffic cannot be policed.

Related Documentation

- [Overview of Policers on page 61](#)

Monitoring Firewall Filter Traffic

You can use operational mode commands to monitor firewall filter traffic.

- [Monitoring Traffic for All Firewall Filters and Policers That Are Configured on page 49](#)
- [Monitoring Traffic for a Specific Firewall Filter on page 50](#)
- [Monitoring Traffic for a Specific Policer on page 50](#)

Monitoring Traffic for All Firewall Filters and Policers That Are Configured

Purpose Monitor the number of packets and bytes that matched the firewall filters and monitor the number of packets that exceeded policer rate limits:

Action Use the **show firewall** operational mode command:

```
user@switch> show firewall
Filter: egress-vlan-watch-employee
Counters:
Name                                     Bytes      Packets
counter-employee-web                    3348        27
Filter: ingress-port-limit-tcp-icmp
Counters:
Name                                     Bytes      Packets
icmp-counter                            560         10
Policers:
Name                                     Packets
icmp-connection-policer                  10
tcp-connection-policer                    0
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```

Meaning The **show firewall** command displays the names of all firewall filters, counters, and policers that are configured. For each counter that is specified in a filter configuration,

the output field shows the byte count and packet count for the term in which the counter is specified. For each policer that is specified in a filter configuration, the output field shows the packet count for packets that exceed the specified rate limits.

Monitoring Traffic for a Specific Firewall Filter

Purpose Monitor the number of packets and bytes that matched a firewall filter and monitor the number of packets that exceeded policer rate limits.

Action Use the **show firewall filter *filter-name*** operational mode command:

```
user@switch> show firewall filter ingress-port-limit-tcp-icmp
Filter: ingress-port-limit-tcp-icmp
Counters:
Name                                     Bytes      Packets
icmp-counter                             560         10
```

Meaning The **show firewall filter *filter-name*** command limits the display information to the counters and policers that are defined for the specified filter.

Monitoring Traffic for a Specific Policer

Purpose Monitor the number of packets that exceeded the rate limits of a policer:

Action Use the **show firewall policer *policer-name*** operational mode command:

```
user@switch> show firewall policer icmp-connection-policer
Filter: ingress-port-limit-tcp-icmp
Policers:
Name                                     Packets
icmp-connection-policer                  10
```

Meaning The **show firewall policer *policer-name*** command displays the number of packets that exceeded the rate limits for the specified policer.

Related Documentation

- [Configuring Firewall Filters on page 39](#)
- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82](#)
- [Verifying That Firewall Filters Are Operational on page 50](#)

Verifying That Firewall Filters Are Operational

Purpose Verify that firewall filters are working properly.

Action Use the **show firewall** operational mode command to verify that the firewall filters are working properly:

```
user@switch> show firewall
Filter: egress-vlan-watch-employee
Counters:
Name                                     Bytes      Packets
counter-employee-web                     0           0
```



```
Filter: ingress-port-limit-tcp-icmp
Counters:
Name                               Bytes      Packets
icmp-counter                       560        10
Policers:
Name                               Packets
icmp-connection-policer           10
tcp-connection-policer            0
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```

Meaning The **show firewall** command displays the names of all firewall filters, counters, and policers that are configured. For each counter that is specified in a filter configuration, the output field shows the byte count and packet count for the term in which the counter is specified. In the above example, the **icmp-counter** in the filter **ingress-port-limit-tcp-icmp** shows that the filter matched 10 packets. For each policer that is specified in a filter configuration, the output field shows the packet count for packets that exceed the specified rate limits. The policer **icmp-connection-policer** shows that 10 ICMP packets were policed.

Related Documentation

- [Configuring Firewall Filters on page 39](#)
- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82](#)
- [Monitoring Firewall Filter Traffic on page 49](#)

Troubleshooting Firewall Filter Configuration

Use the following information to troubleshoot your firewall filter configuration.

- [Firewall Filter Configuration Returns a No Space Available in TCAM Message on page 52](#)
- [Filter Counts Previously Dropped Packet on page 53](#)
- [Matching Packets Not Counted on page 54](#)
- [Counter Reset When Editing Filter on page 54](#)
- [Cannot Include loss-priority and policer Actions in Same Term on page 54](#)
- [Cannot Egress Filter Certain Traffic Originating on QFX Switch on page 55](#)
- [Firewall Filter Match Condition Not Working with Q-in-Q Tunneling on page 55](#)
- [Egress Firewall Filters with Private VLANs on page 55](#)
- [Egress Filtering of L2PT Traffic Not Supported on page 56](#)
- [Cannot Drop BGP Packets in Certain Circumstances on page 56](#)
- [Invalid Statistics for Policer on page 57](#)
- [Policers can Limit Egress Filters on page 57](#)

Firewall Filter Configuration Returns a No Space Available in TCAM Message

Problem **Description:** When a firewall filter configuration exceeds the amount of available Ternary Content Addressable Memory (TCAM) space, the system returns the following **syslogd** message:

```
No space available in tcam.  
Rules for filter filter-name will not be installed.
```

A switch returns this message during the commit operation if the firewall filter that has been applied to a port, VLAN, or Layer 3 interface exceeds the amount of space available in the TCAM table. The filter is not applied, but the commit operation for the firewall filter configuration is completed in the CLI module.

Solution When a firewall filter configuration exceeds the amount of available TCAM table space, you must configure a new firewall filter with fewer filter terms so that the space requirements for the filter do not exceed the available space in the TCAM table.

You can perform either of the following procedures to correct the problem:

To delete the filter and its binding and apply the new smaller firewall filter to the same binding:

1. Delete the filter and its binding to ports, VLANs, or Layer 3 interfaces. For example:

```
[edit]  
user@switch# delete firewall family ethernet-switching filter ingress-vlan-rogue-block  
user@switch# delete vlans employee-vlan description "filter to block rogue devices on  
employee-vlan"  
user@switch# delete vlans employee-vlan filter input ingress-vlan-rogue-block
```

2. Commit the changes:

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

3. Configure a smaller filter with fewer terms that does not exceed the amount of available TCAM space. For example:

```
[edit]  
user@switch# set firewall family ethernet-switching filter new-ingress-vlan-rogue-block ...
```

4. Apply (bind) the new firewall filter to a port, VLAN, or Layer 3 interface. For example:

```
[edit]  
user@switch# set vlans employee-vlan description "filter to block rogue devices on  
employee-vlan"  
user@switch# set vlans employee-vlan filter input new-ingress-vlan-rogue-block
```

5. Commit the changes:

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

To apply a new firewall filter and overwrite the existing binding but not delete the original filter:

1. Configure a firewall filter with fewer terms than the original filter:

```
[edit]  
user@switch# set firewall family ethernet-switching filter new-ingress-vlan-rogue-block...
```

2. Apply the firewall filter to the port, VLAN, or Layer 3 interfaces to overwrite the binding of the original filter—for example:

```
[edit]
user@switch# set vlans employee-vlan description "smaller filter to block rogue devices on employee-vlan"
```

```
user@switch# set vlans employee-vlan filter input new-ingress-vlan-rogue-block
```

Because you can apply no more than one firewall filter per VLAN per direction, the binding of the original firewall filter to the VLAN is overwritten with the new firewall filter **new-ingress-vlan-rogue-block**.

3. Commit the changes:

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



NOTE: The original filter is not deleted and is still available in the configuration.

Filter Counts Previously Dropped Packet

Problem Description: If you configure two or more filters in the same direction for a physical interface and one of the filters includes a counter, the counter will be incorrect if the following circumstances apply:

- You configure the filter that is applied to packets first to discard certain packets. For example, imagine that you have a VLAN filter that accepts packets sent to 10.10.1.0/24 addresses and implicitly discards packets sent to any other addresses. You apply the filter to the **admin** VLAN in the output direction, and interface xe-0/0/1 is a member of that VLAN.
- You configure a subsequent filter to accept and count packets that are dropped by the first filter. In this example, you have a port filter that accepts and counts packets sent to 192.168.1.0/24 addresses that is also applied to xe-0/0/1 in the output direction.

The egress VLAN filter is applied first and correctly discards packets sent to 192.168.1.0/24 addresses. The egress port filter is applied next and counts the discarded packets as matched packets. The packets are not forwarded, but the counter displayed by the egress port filter is incorrect.

Remember that the order in which filters are applied depends on the direction in which they are applied, as indicated here:

Ingress filters:

1. Port (Layer 2) filter
2. VLAN filter
3. Router (Layer 3) filter

Egress filters:

1. Router (Layer 3) filter
2. VLAN filter
3. Port (Layer 2) filter

Solution This is expected behavior.

Matching Packets Not Counted

Problem **Description:** If you configure two egress filters with counters for a physical interface and a packet matches both of the filters, only one of the counters includes that packet. For example:

- You configure an egress port filter with a counter for interface xe-0/0/1.
- You configure an egress VLAN filter with a counter for the **adminVLAN**, and interface xe-0/0/1 is a member of that VLAN.
- A packet matches both filters.

In this case, the packet is counted by only one of the counters even though it matched both filters.

Solution This is expected behavior.

Counter Reset When Editing Filter

Problem **Description:** If you edit a firewall filter term, the value of any counter associated with any term in the same filter is set to 0, including the implicit counter for any policer referenced by the filter. Consider the following examples:

- Assume that your filter has **term1**, **term2**, and **term3**, and each term has a counter that has already counted matching packets. If you edit any of the terms in any way, the counters for all the terms are reset to 0.
- Assume that your filter has **term1** and **term2**. Also assume that **term2** has a **policer** action modifier and the implicit counter of the policer has already counted 1000 matching packets. If you edit **term1** or **term2** in any way, the counter for the policer referenced by **term2** is reset to 0.

Solution This is expected behavior.

Cannot Include loss-priority and policer Actions in Same Term

Problem **Description:** You cannot include both of the following actions in the same firewall filter term in a QFX Series switch:

- **loss-priority**
- **policer**

If you do so, you see the following error message when you attempt to commit the configuration: "cannot support policer action if loss-priority is configured."

Solution This is expected behavior.

Cannot Egress Filter Certain Traffic Originating on QFX Switch

Problem Description: On a QFX Series switch, you cannot filter certain traffic with a firewall filter applied in the output direction if the traffic originates on the QFX switch. This limitation applies to control traffic for protocols such as ICMP (ping), STP, LACP, and so on.

Solution This is expected behavior.

Firewall Filter Match Condition Not Working with Q-in-Q Tunneling

Problem Description: If you create a firewall filter that includes a match condition of **dot1q-tag** or **dot1q-user-priority** and apply the filter on input to a trunk port that participates in a service VLAN, the match condition does not work if the Q-in-Q EtherType is not 0x8100. (When Q-in-Q tunneling is enabled, trunk interfaces are assumed to be part of the service provider or data center network and therefore participate in service VLANs.)

Solution This is expected behavior. To set the Q-in-Q EtherType to 0x8100, enter the **set dot1q-tunneling ethertype 0x8100** statement at the **[edit ethernet-switching-options]** hierarchy level. You must also configure the other end of the link to use the same Ethertype.

Egress Firewall Filters with Private VLANs

Problem Description: If you apply a firewall filter in the output direction to a primary VLAN, the filter also applies to the secondary VLANs that are members of the primary VLAN when the traffic egresses with the primary VLAN tag or isolated VLAN tag, as listed below:

- Traffic forwarded from a secondary VLAN trunk port to a promiscuous port (trunk or access)
- Traffic forwarded from a secondary VLAN trunk port that carries an isolated VLAN to a PVLAN trunk port.
- Traffic forwarded from a promiscuous port (trunk or access) to a secondary VLAN trunk port
- Traffic forwarded from a PVLAN trunk port. to a secondary VLAN trunk port
- Traffic forwarded from a community port to a promiscuous port (trunk or access)

If you apply a firewall filter in the output direction to a primary VLAN, the filter does *not* apply to traffic that egresses with a community VLAN tag, as listed below:

- Traffic forwarded from a community trunk port to a PVLAN trunk port
- Traffic forwarded from a secondary VLAN trunk port that carries a community VLAN to a PVLAN trunk port
- Traffic forwarded from a promiscuous port (trunk or access) to a community trunk port
- Traffic forwarded from a PVLAN trunk port. to a community trunk port

If you apply a firewall filter in the output direction to a community VLAN, the following behaviors apply:

- The filter is applied to traffic forwarded from a promiscuous port (trunk or access) to a community trunk port (because the traffic egresses with the community VLAN tag).
- The filter is applied to traffic forwarded from a community port to a PVLAN trunk port (because the traffic egresses with the community VLAN tag).
- The filter is *not* applied to traffic forwarded from a community port to a promiscuous port (because the traffic egresses with the primary VLAN tag or untagged).

Solution These are expected behaviors. They occur only if you apply a firewall filter to a private VLAN in the output direction and do not occur if you apply a firewall filter to a private VLAN in the input direction.

Egress Filtering of L2PT Traffic Not Supported

Problem **Description:** Egress filtering of L2PT traffic is not supported on the QFX3500 switch. That is, if you configure L2PT to tunnel a protocol on an interface, you cannot also use a firewall filter to filter traffic for that protocol on that interface in the output direction. If you commit a configuration for this purpose, the firewall filter is not applied to the L2PT-tunneled traffic.

Solution This is expected behavior.

Cannot Drop BGP Packets in Certain Circumstances

Problem **Description:** BGP packets with a time-to-live (TTL) value greater than 1 cannot be discarded using a firewall filter applied to a loopback interface or applied on input to a Layer 3 interface. BGP packets with TTL value of 1 or 0 can be discarded using a firewall filter applied to a loopback interface or applied on input to a Layer 3 interface.

Solution This is expected behavior.

Invalid Statistics for Policer

Problem **Description:** If you apply a single-rate two-color policer in more than 128 terms in a firewall filter, the output of the **show firewall** command displays incorrect data for the policer.

Solution This is expected behavior.

Policers can Limit Egress Filters

Problem **Description:** The number of egress policers that you configure can affect the total number of allowed egress firewall filters. Every policer has two implicit counters that consume two entries in a 1024-entry TCAM that is used for counters, including counters that are configured as action modifiers in firewall filter terms. (Policers consume two entries because one is used for green packets and one is used for nongreen packets regardless of policer type.) If the TCAM becomes full, you cannot commit any more egress firewall filters that have terms with counters. For example, if you configure and commit 512 egress policers (two-color, three-color, or a combination of both policer types), all of the memory entries for counters are used up. If later in your configuration file you insert additional egress firewall filters with terms that also include counters, *none* of the terms in those filters are committed because there is no available memory space for the counters. Here are some additional examples:

- Assume that you configure egress filters that include a total of 512 policers and no counters. Later in your configuration file you include another egress filter with 10 terms, 1 of which has a counter action modifier. None of the terms in this filter are committed because there is not enough TCAM space for the counter.
- Assume that you configure egress filters that include a total of 500 policers, so 1000 TCAM entries are occupied. Later in your configuration file you include the following two egress filters:
 - Filter A with 20 terms and 20 counters. All the terms in this filter are committed because there is enough TCAM space for all the counters.
 - Filter B comes after Filter A and has five terms and five counters. *None* of the terms in this filter are committed because there is not enough memory space for *all* the counters. (Five TCAM entries are required but only four are available.)

Solution You can prevent this problem by ensuring that egress firewall filter terms with counter actions are placed earlier in your configuration file than terms that include policers. In this circumstance, Junos OS commits policers even if there is not enough TCAM space for the implicit counters. For example, assume the following:

- You have 1024 egress firewall filter terms with counter actions.
- Later in your configuration file you have an egress filter with 10 terms. None of the terms have counters but one has a policer action modifier.

You can successfully commit the filter with 10 terms even though there is not enough TCAM space for the implicit counters of the policer. The policer is committed without the counters.

**Related
Documentation**

- *Understanding FIP Snooping, FBF, and MVR Filter Scalability*
- [Configuring Firewall Filters on page 39](#)
- [Verifying That Firewall Filters Are Operational on page 50](#)

PART 2

Policers

- [Using Policers on page 61](#)

CHAPTER 2

Using Policers

- [Overview of Policers on page 61](#)
- [Understanding Policers with Link Aggregation Groups on page 67](#)
- [Understanding Color-Blind Mode for Single-Rate Tricolor Marking on page 67](#)
- [Understanding Color-Aware Mode for Single-Rate Tricolor Marking on page 68](#)
- [Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 69](#)
- [Understanding Color-Aware Mode for Two-Rate Tricolor Marking on page 70](#)
- [Understanding Policers on OVSDb-Managed Interfaces on page 72](#)
- [Example: Applying a Policer to OVSDb-Managed Interfaces on page 72](#)
- [Example: Using Two-Color Policers and Prefix Lists on page 75](#)
- [Example: Using Policers to Manage Oversubscription on page 78](#)
- [Assigning Forwarding Classes and Loss Priority on page 80](#)
- [Configuring Color-Blind Egress Policers for Medium-Low PLP on page 82](#)
- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82](#)
- [Verifying That Three-Color Policers Are Operational on page 84](#)
- [Verifying That Two-Color Policers Are Operational on page 85](#)
- [Troubleshooting Policer Configuration on page 85](#)

Overview of Policers

A switch polices traffic by limiting the input or output transmission rate of a class of traffic according to user-defined criteria. Policing (or rate-limiting) traffic allows you to control the maximum rate of traffic sent or received on an interface and to provide multiple priority levels or classes of service.

- [Policer Overview on page 62](#)
- [Policer Types on page 62](#)
- [Policer Actions on page 63](#)
- [Policer Colors on page 64](#)
- [Filter-Specific Policers on page 64](#)
- [Suggested Naming Convention for Policers on page 65](#)

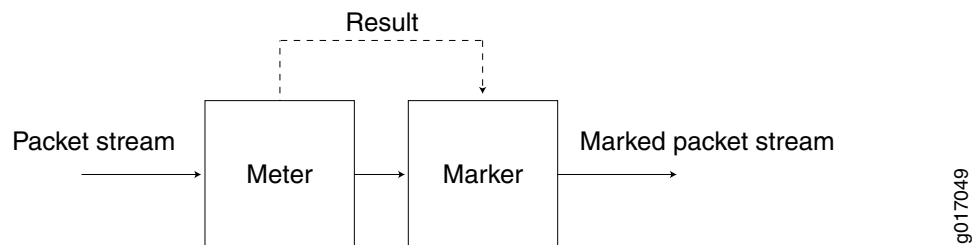
- [Policer Counters on page 65](#)
- [Policer Algorithms on page 65](#)
- [How Many Policers Are Supported? on page 65](#)
- [Policers Can Limit Egress Firewall Filters on page 66](#)

Policer Overview

You use policers to apply limits to traffic flow and set consequences for packets that exceed these limits—usually applying a higher loss priority—so that if packets encounter downstream congestion, they can be discarded first. Policers apply only to unicast packets.

Policers provide two functions: metering and marking. A policer meters (measures) each packet against traffic rates and burst sizes that you configure. It then passes the packet and the metering result to the marker, which assigns a packet loss priority that corresponds to the metering result. [Figure 3 on page 62](#) illustrates this process.

Figure 3: Flow of Tricolor Marking Policer Operation



After you name and configure a policer, you use it by specifying it as an action in one or more firewall filters.

Policer Types

A switch supports three types of policers:

- **Single-rate two-color marker**—A two-color policer (or “policer” when used without qualification) meters the traffic stream and classifies packets into two categories of packet loss priority (PLP) according to a configured bandwidth and burst-size limit. You can mark packets that exceed the bandwidth and burst-size limit with a specified PLP or simply discard them.

You can specify this type of policer in an ingress or egress firewall.



NOTE: A two-color policer is most useful for metering traffic at the port (physical interface) level.

- **Single-rate three-color marker**—This type of policer is defined in RFC 2697, *A Single Rate Three Color Marker*, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on one rate—the configured committed information rate (CIR) as well as the committed burst size (CBS) and the excess burst size (EBS). The CIR specifies the average rate at which bits are admitted to the switch. The CBS

specifies the usual burst size in bytes and the EBS specifies the maximum burst size in bytes. The EBS must be greater than or equal to the CBS, and neither can be 0.

You can specify this type of policer in an ingress or egress firewall.



NOTE: A single-rate three-color marker (TCM) is most useful when a service is structured according to packet length and not peak arrival rate.

- Two-rate three-color marker—This type of policer is defined in RFC 2698, *A Two Rate Three Color Marker*, as part of an assured forwarding per-hop-behavior classification system for a Differentiated Services environment. This type of policer meters traffic based on two rates—the CIR and peak information rate (PIR) along with their associated burst sizes, the CBS and peak burst size (PBS). The PIR specifies the maximum rate at which bits are admitted to the network and must be greater than or equal to the CIR.

You can specify this type of policer in an ingress or egress firewall.



NOTE: A two-rate three-color policer is most useful when a service is structured according to arrival rates and not necessarily packet length.

See [Table 8 on page 63](#) for information about how metering results are applied for each of these policer types.

Policer Actions

Policer actions are implicit or explicit and vary by policer type. *Implicit* means that Junos OS assigns the loss priority automatically. [Table 8 on page 63](#) describes the policer actions.

Table 8: Policer Actions

Policer	Marking	Implicit Action	Configurable Action
Single-rate two-color	Green (conforming)	Assign low loss priority	None
	Red (nonconforming)	None	Discard
Single-rate three-color	Green (conforming)	Assign low loss priority	None
	Yellow (above the CIR and CBS)	Assign medium-high loss priority	None
	Red (above the EBS)	Assign high loss priority	Discard

Table 8: Policer Actions (*continued*)

Policer	Marking	Implicit Action	Configurable Action
Two-rate three-color	Green (conforming)	Assign low loss priority	None
	Yellow (above the CIR and CBS)	Assign medium-high loss priority	None
	Red (above the PIR and PBS)	Assign high loss priority	Discard



NOTE: If you specify a policer in an egress firewall filter, the only supported action is **discard**.

Policer Colors

Single-rate and two-rate three-color policers can operate in two modes:

- **Color-blind**—In color-blind mode, the three-color policer assumes that all packets examined have not been previously marked or metered. In other words, the three-color policer is “blind” to any previous coloring a packet might have had.
- **Color-aware**—In color-aware mode, the three-color policer assumes that all packets examined have been previously marked or metered. In other words, the three-color policer is “aware” of the previous coloring a packet might have had. In color-aware mode, the three-color policer can increase the PLP of a packet but cannot decrease it. For example, if a color-aware three-color policer meters a packet with a medium PLP marking, it can raise the PLP level to high but cannot reduce the PLP level to low.

Filter-Specific Policers

You can configure policers to be filter-specific, which means that Junos OS creates only one policer instance regardless of how many times the policer is referenced. When you do this, rate limiting is applied in aggregate, so if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, the total bandwidth allowed by the filter is 1 Gbps. However, the behavior of a filter-specific policer is affected by how the firewall filter terms that reference the policer are stored in TCAM. If you create a filter-specific policer and reference it in multiple firewall filter terms, the policer allows more traffic than expected if the terms are stored in different TCAM slices. For example, if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms that are stored in three separate memory slices, the total bandwidth allowed by the filter is 3 Gbps, not 1 Gbps.

To prevent this unexpected behavior from occurring, use the information about TCAM slices presented in [“Planning the Number of Firewall Filters to Create” on page 34](#) to organize your configuration file so that all the firewall filter terms that reference a given filter-specific policer are stored in the same TCAM slice.

Suggested Naming Convention for Policers

We recommend that you use the naming convention ***policertypeTCM#-color type*** when configuring three-color policers and ***policer#*** when configuring two-color policers. TCM stands for three-color marker. Because policers can be numerous and must be applied correctly to work, a simple naming convention makes it easier to apply the policers properly. For example, the first single-rate, color-aware three-color policer configured would be named **srTCM1-ca**. The second two-rate, color-blind three-color configured would be named **trTCM2-cb**. The elements of this naming convention are explained below:

- sr (single-rate)
- tr (two-rate)
- TCM (tricolor marking)
- 1 or 2 (number of marker)
- ca (color-aware)
- cb (color-blind)

Policer Counters

Each policer that you configure includes an implicit counter that counts the number of packets that exceed the rate limits that are specified for the policer. If you use the same policer in multiple terms—either within the same filter or in different filters—the implicit counter counts all the packets that are policed in all of these terms. If you want to obtain separate packet counts for each term, use these options:

- Configure a unique policer for each term.
- Configure only one policer, but use a unique, explicit counter in each term.

Policer Algorithms

Policing uses the *token-bucket algorithm*, which enforces a limit on average bandwidth while allowing bursts up to a specified maximum value. It offers more flexibility than the *leaky bucket algorithm* in allowing a certain amount of bursty traffic before it starts discarding packets.

How Many Policers Are Supported?

QFX5100 switches support 1535 ingress policers and 1024 egress policers (assuming one policer per firewall filter term).

QFX3500 and QFX3600 standalone switches and QFabric Node devices support the following numbers of policers (assuming one policer per firewall filter term):

- Two-color policers used in ingress firewall filters: 767
- Three-color policers used in ingress firewall filters: 767

- Two-color policers used in egress firewall filters: 1022
- Three-color policers used in egress firewall filters: 512

Policers Can Limit Egress Firewall Filters

The number of egress policers that you configure can affect the total number of allowed egress firewall filters. Every policer has two implicit counters that consume two entries in a 1024-entry TCAM that is used for counters, including counters that are configured as action modifiers in firewall filter terms. (Policers consume two entries because one is used for green packets and one is used for nongreen packets regardless of policer type.) If the TCAM becomes full, you cannot commit any more egress firewall filters that have terms with counters. For example, if you configure and commit 512 egress policers (two-color, three-color, or a combination of both policer types), all of the memory entries for counters are used up. If later in your configuration file you insert additional egress firewall filters with terms that also include counters, *none* of the terms in those filters are committed because there is no available memory space for the counters.

Here are some additional examples:

- Assume that you configure egress filters that include a total of 512 policers and no counters. Later in your configuration file you include another egress filter with 10 terms, 1 of which has a counter action modifier. None of the terms in this filter are committed because there is not enough TCAM space for the counter.
- Assume that you configure egress filters that include a total of 500 policers, so 1000 TCAM entries are occupied. Later in your configuration file you include the following two egress filters:
 - Filter A with 20 terms and 20 counters. All the terms in this filter are committed because there is enough TCAM space for all the counters.
 - Filter B comes after Filter A and has five terms and five counters. *None* of the terms in this filter are committed because there is not enough memory space for *all* the counters. (Five TCAM entries are required but only four are available.)

You can prevent this problem by ensuring that egress firewall filter terms with counter actions are placed earlier in your configuration file than terms that include policers. In this circumstance, Junos OS commits policers even if there is not enough TCAM space for the implicit counters. For example, assume the following:

- You have 1024 egress firewall filter terms with counter actions.
- Later in your configuration file you have an egress filter with 10 terms. None of the terms have counters but one has a policer action modifier.

You can successfully commit the filter with 10 terms even though there is not enough TCAM space for the implicit counters of the policer. The policer is committed without the counters.

Related Documentation

- [Understanding Color-Blind Mode for Single-Rate Tricolor Marking on page 67](#)
- [Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 69](#)

- [Understanding Color-Aware Mode for Single-Rate Tricolor Marking on page 68](#)
- [Understanding Color-Aware Mode for Two-Rate Tricolor Marking on page 70](#)
- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82](#)

Understanding Policers with Link Aggregation Groups

If you apply a policer to a link aggregation group (LAG) on a standalone switch or QFabric node, the policer applies to all the interfaces in the LAG in aggregate. For example, if you configure a policer to rate-limit at 1 Gbps and apply the policer (by using a firewall filter) to a LAG that has two member interfaces on a single switch or node, the total allowed throughput for both members is 1 Gbps.

If you apply a policer to a LAG that has members on different nodes in a QFabric network Node group or redundant server Node group, the configured rate applies to the interface on each node. For example, if you configure a policer to rate-limit at 1 Gbps and apply the policer to a LAG that has one member on server node A and one member on server node B, the allowed throughput for each member is 1 Gbps, for a total allowed throughput of 2 Gbps.

Related Documentation

- [Overview of Policers on page 61](#)
- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82](#)

Understanding Color-Blind Mode for Single-Rate Tricolor Marking

With the color-blind mode of single-rate tricolor marking, all packets are evaluated against the CBS. If a packet exceeds the CBS, it is evaluated against the EBS. In color-blind mode, the policer supports three loss priorities only: low, medium-high, and high.

Packets that exceed the CBS but are below the EBS are marked yellow (medium-high). Packets that exceed the EBS are marked red (high), as shown in [Table 9 on page 67](#).

Table 9: Color-Blind Mode TCM Color-to-PLP Mapping

Color	PLP	Meaning
Green	low	Conforming.
Yellow	medium-high	Packet exceeds the CIR and CBS but does not exceed the EBS.
Red	high	Packet exceeds the EBS.

Related Documentation

- [Overview of Policers on page 61](#)
- [Configuring Color-Blind Egress Policers for Medium-Low PLP on page 82](#)

Understanding Color-Aware Mode for Single-Rate Tricolor Marking

In color-aware mode, the treatment the packet receives depends on its classification. Marking can increase a preassigned PLP but cannot decrease it.

Summary of PLP Changes

Table 10 on page 68 shows how a packet's incoming priority can be modified with single-rate marking.

Table 10: Color-Aware Mode Single-Rate PLP Mapping

Incoming PLP	Packet Metered Against	Possible Cases	Outgoing PLP
low	CIR, CBS, and EBS	Conforming	low
		Packet exceeds the CIR and CBS but does not exceed the EBS.	medium-high
		Packet exceeds the EBS.	high
medium-low	EBS only	Packet does not exceed the EBS.	medium-low
		Packet exceeds the EBS.	high
medium-high	EBS only	Packet does not exceed the EBS.	medium-high
		Packet exceeds the EBS.	high
high	Not metered by the policer.	All cases.	high

The following sections describe single-rate color-aware PLP mapping in more detail.

Effect on Green Packets (Low PLP)

Packets belonging to the green class have already been marked by a classifier with low PLP. The marking policer can leave the PLP unchanged or increase it to medium-high or high, so these packets are therefore metered against both the CBS and the EBS. For example, if a behavior aggregate or multifield classifier marks a packet with low PLP and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CIR, packets remain marked as low PLP.
- If bursts exceed the CBS but not the EBS, some of the packets are marked as medium-high PLP, and some of the packets remain marked as low PLP.
- If bursts exceed the EBS, some of the packets are marked as high PLP, and some of the packets remain marked as low PLP.

Effect on Yellow Packets (Medium PLP)

Packets belonging to the yellow class have already been marked by a classifier with medium-low or medium-high PLP. The marking policer can leave the PLP unchanged or increase it to high, so these packets are therefore metered against the EBS only. For example, if a behavior aggregate or multifield classifier marks a packet with medium-low PLP and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CBS, the packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the CBS but less than the EBS, the packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the EBS, some of the packets are marked as high PLP and some remain marked as medium-low PLP.

If a BA or multifield classifier marks a packet with medium-high PLP and the two-rate TCM policer is in color-aware mode, the policer assigns output loss priority as follows:

- If the rate of traffic flow is less than the CBS, the packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the CBS but less than the EBS, the packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the EBS, some of the packets are marked as high PLP and some remain marked as medium-high PLP.

Effect on Red Packets (High PLP)

Packets belonging to the red class have already been marked by a classifier with high PLP. Because the policer cannot decrease the PLP, it does not change it, and these packets are not metered against the CBS or the EBS.

Related Documentation

- [Overview of Policers on page 61](#)
- [Configuring Color-Blind Egress Policers for Medium-Low PLP on page 82](#)

Understanding Color-Blind Mode for Two-Rate Tricolor Marking

With the color-blind mode of two-rate tricolor marking, all packets are evaluated against the committed information rate (CIR). If a packet exceeds the CIR, it is evaluated against the peak information rate (PIR). Packets that exceed the CIR but are below the PIR are marked yellow (medium-high). Packets that exceed the PIR are marked red (high).

Table 11: Color-Blind Mode TCM Color-to-PLP Mapping

Color	PLP	Meaning
Green	low	Packet does not exceed the CIR.

Table 11: Color-Blind Mode TCM Color-to-PLP Mapping (*continued*)

Color	PLP	Meaning
Yellow	medium-high	Packet exceeds the CIR but does not exceed the PIR.
Red	high	Packet exceeds the PIR.

Related Documentation

- [Overview of Policers on page 61](#)
- [Configuring Color-Blind Egress Policers for Medium-Low PLP on page 82](#)

Understanding Color-Aware Mode for Two-Rate Tricolor Marking

In color-aware mode, the treatment the packet receives depends on its classification. Marking can increase the preassigned PLP but cannot decrease it.

Summary of PLP Changes

Table 12 on page 70 shows how a packet's incoming priority can be modified with two-rate marking.

Table 12: Color-Aware Mode Two-Rate PLP Mapping

Incoming PLP	Packet Metered Against	Possible Cases	Outgoing PLP
low	CIR and PIR	Packet does not exceed the CIR.	low
		Packet exceeds the CIR but not the PIR.	medium-high
		Packet exceeds the PIR.	high
medium-low	PIR only	Packet does not exceed the PIR.	medium-low
		Packet exceeds the PIR.	high
medium-high	PIR only	Packet does not exceed the PIR.	medium-high
		Packet exceeds the PIR.	high
high	Not metered by the policer.	All cases.	high

The following sections describe color-aware two-rate PLP mapping in more detail.

Effect on Green Packets (Low PLP)

Packets belonging to the green class have already been marked by a classifier with low PLP. The marking policer can leave the packet's PLP unchanged or increase the PLP to medium-high or high. These packets are therefore metered against both the CIR and the

PIR. For example, if a behavior aggregate or multifield classifier marks a packet with low PLP and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CIR, the packets remain marked as low PLP.
- If the rate of traffic flow is greater than the CIR but less than the PIR, some of the packets are marked as medium-high PLP and some of the packets remain marked as low PLP.
- If the rate of traffic flow is greater than the PIR, some of the packets are marked as high PLP and some of the packets remain marked as low PLP.

Effect on Yellow Packets (Medium PLP)

Packets belonging to the yellow class have already been marked by a classifier with medium-low or medium-high PLP. The marking policer can leave the PLP unchanged or increase it to high. These packets are therefore metered against the PIR only. For example, if a behavior aggregate (BA) or multifield classifier marks a packet with medium-low PLP and the two-rate TCM policer is in color-aware mode, the policer assigns output loss priority as follows:

- If the rate of traffic flow is less than the CIR, the packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the CIR but less than the PIR, the packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the PIR, some of the packets are marked as high PLP and some of the packets remain marked as medium-low PLP.

If a BA or multifield classifier marks a packet with medium-high PLP and the two-rate TCM policer is in color-aware mode, the policer assigns output loss priority as follows:

- If the rate of traffic flow is less than the CIR, the packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the CIR but less than the PIR, the packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the PIR, some of the packets are marked as high PLP and some of the packets remain marked as medium-high PLP.

Effect on Red Packets (High PLP)

Packets belonging to the red class have already been marked by a classifier with high PLP. Because the policer cannot decrease the PLP, it does not change it, and these packets are not metered against the CIR or the PIR.

Related Documentation

- [Overview of Policers on page 61](#)
- [Configuring Color-Blind Egress Policers for Medium-Low PLP on page 82](#)

Understanding Policers on OVSDB-Managed Interfaces

When you use a Contrail controller to manage VXLANs on a QFX switch (through the Open vSwitch Database—OVSDB—management protocol), the VXLAN interfaces are automatically configured with the **flexible-vlan-tagging** and **encapsulation extended-vlan-bridge** statements. Starting with Junos OS Release 14.1X53-D30, you can create **family ethernet-switching** logical units (subinterfaces) on these interfaces. This enables you to apply firewall filters with the action **three-color-policer** to these subinterfaces, which means that you can apply two-rate three-color markers (policers) to OVSDB-managed interfaces. See [“Example: Applying a Policer to OVSDB-Managed Interfaces” on page 72](#) for information about how to configure policers on VXLAN interfaces managed by a Contrail controller.



NOTE: Firewall filters are the only supported configuration items on **family ethernet-switching** subinterfaces of OVSDB-managed interfaces. Two-rate three-color markers are the only supported policers.

Related Documentation

- [Example: Applying a Policer to OVSDB-Managed Interfaces on page 72](#)
- [Overview of Policers on page 61](#)
- [Understanding VXLANs](#)
- [Understanding the OVSDB Protocol Running on Juniper Networks Devices](#)
- [Understanding Firewall Filters on OVSDB-Managed Interfaces on page 5](#)

Example: Applying a Policer to OVSDB-Managed Interfaces

Starting with Junos OS Release 14.1X53-D30, you can create **family ethernet-switching** logical units (subinterfaces) on VXLAN interfaces managed by a Contrail controller. (The controller and switch communicate through the Open vSwitch Database—OVSDB—management protocol). This support enables you to apply firewall filters with the action **three-color-policer** to these subinterfaces, which means that you can apply two-rate three-color markers (policers) to OVSDB-managed interfaces.

Because a Contrail controller can create subinterfaces dynamically, you need to apply firewall filters in such a way that the filters will apply to subinterfaces whenever the controller creates them. You accomplish this by using configuration groups to configure and apply the firewall filters. (You must use configuration groups for this purpose—that is, you cannot apply a firewall filter directly to these subinterfaces.)



NOTE: Firewall filters are the only supported configuration items on family ethernet-switching subinterfaces of OVSDB-managed interfaces. Two-rate three-color markers are the only supported policers.

- [Requirements on page 73](#)
- [Overview on page 73](#)
- [Configuration on page 73](#)

Requirements

This example uses the following hardware and software components:

- A QFX5100 switch
- Junos OS Release 14.1X53-D30 or later

Overview

This example assumes that interfaces xe-0/0/0 and xe-0/0/1 on the switch are VXLAN interfaces managed by a Contrail controller, which means that the controller has applied the **flexible-vlan-tagging** and **encapsulation extended-vlan-bridge** statements to these interfaces. To apply a firewall filter Layer 2 (port) firewall filter with a policer action to any subinterfaces that the controller creates dynamically, you must create and apply the filter as shown in this example.



NOTE: As shown in the example, all of the statements must be part of a configuration group when you want to apply a firewall filter (and policer) to an OVSDB-managed subinterface.

Configuration

To configure a firewall filter with a policer action to be automatically applied to subinterfaces created dynamically by a Contrail controller, perform these tasks:

CLI Quick Configuration	<pre> [edit] set groups vxlan-policer-group interfaces xe-0/0/0 unit <*> family ethernet-switching filter input vxlan-filter set groups vxlan-policer-group interfaces xe-0/0/1 unit <*> family ethernet-switching filter input vxlan-filter set groups vxlan-policer-group firewall three-color-policer vxlan-policer action loss-priority high then discard set groups vxlan-policer-group firewall three-color-policer vxlan-policer two-rate color-blind set groups vxlan-policer-group firewall three-color-policer vxlan-policer two-rate committed-burst-size 2m set groups vxlan-policer-group firewall three-color-policer vxlan-policer two-rate committed-information-rate 100m set groups vxlan-policer-group firewall three-color-policer vxlan-policer two-rate peak-burst-size 4m set groups vxlan-policer-group firewall three-color-policer vxlan-policer two-rate peak-information-rate 100m set groups vxlan-policer-group firewall family ethernet-switching filter vxlan-filter term t1 then three-color-policer two-rate vxlan-policer set apply-groups vxlan-policer-group </pre>
Step-by-Step Procedure	<ol style="list-style-type: none"> 1. Create configuration group vxlan-policer-group to apply firewall filter vxlan-filter to any subinterface of interface xe-0/0/0. The filter applies to any subinterface because you specify unit <*>: <pre> [edit] user@switch# set groups vxlan-policer-group interfaces xe-0/0/0 unit <*> family ethernet-switching filter input vxlan-filter </pre> 2. Create the same configuration for interface xe-0/0/1: <pre> [edit] user@switch# set groups vxlan-policer-group interfaces xe-0/0/1 unit <*> family ethernet-switching filter input vxlan-filter </pre> 3. Configure the policer to discard packets with high loss priority. (Junos OS assigns high loss priority to packets that exceed the peak information rate and the peak burst size.) As with the interface configuration, you must also configure the policer to be part of a configuration group. <pre> [edit] user@switch# set groups vxlan-policer-group firewall three-color-policer vxlan-policer action loss-priority high then discard </pre> 4. Configure the policer to be color blind, which means that it ignores any preclassification of packets and can assign a higher or lower packet loss priority. <pre> [edit] user@switch# set groups vxlan-policer-group firewall three-color-policer vxlan-policer two-rate color-blind </pre> 5. Configure the policer to allow incoming traffic to burst a maximum of 2 megabytes above the committed information rate and still be marked with low packet loss priority (green). <pre> [edit] user@switch# set groups vxlan-policer-group firewall three-color-policer vxlan-policer two-rate committed-burst-size 2m </pre> 6. Configure the policer to allow guaranteed bandwidth of 100 megabytes under normal line conditions. This is the average rate up threshold under which packets are marked with low packet loss priority (green). <pre> [edit] </pre>

- ```
user@switch# set groups vxlan-policer-group firewall three-color-policer vxlan-policer
two-rate committed-information-rate 100m
```
7. Configure the policer to allow incoming packets to burst a maximum of 4 megabytes above the peak information rate and still be marked with medium-high packet loss priority (yellow). Packets that exceed the peak burst size are marked with high packet loss priority (red).
 

```
[edit]
user@switch# set groups vxlan-policer-group firewall three-color-policer vxlan-policer
two-rate peak-burst-size 4m
```
  8. Configure the policer to allow a maximum achievable rate of 100 megabytes. Packets that exceed the committed information rate but are below the peak information rate are marked with medium-high packet loss priority (yellow). Packets that exceed the peak information rate are marked with high packet loss priority (red).
 

```
[edit]
user@switch# set groups vxlan-policer-group firewall three-color-policer vxlan-policer
two-rate peak-information-rate 100m
```
  9. Configure the firewall filter **vxlan-filter** to send matching packets (all packets, because there is no **from** statement) to the policer:
 

```
[edit]
user@switch# set groups vxlan-policer-group firewall family ethernet-switching filter
vxlan-filter term t1 then three-color-policer two-rate vxlan-policer
```
  10. Apply the group to enable its configuration:
 

```
[edit]
user@switch# set apply-groups vxlan-policer-group
```

#### Related Documentation

- [Understanding Junos OS Configuration Groups](#)
- [Overview of Firewall Filters on page 3](#)
- [Overview of Policers on page 61](#)
- [Understanding VXLANs](#)
- [Understanding the OVSDb Protocol Running on Juniper Networks Devices](#)
- [Understanding Policers on OVSDb-Managed Interfaces on page 72](#)

## Example: Using Two-Color Policers and Prefix Lists

If you provide specific amounts of bandwidth to internal or external customers, you can use policing to make sure that customers do not consume more bandwidth than they should receive. For example, you might connect many customers to one 10-Gbps interface and want to ensure that none of them congest the interface by using more bandwidth than they have been allotted.

You could accomplish this by creating a two-color policer similar to the following for each customer:

```
firewall {
 policer Limit-Customer-1 {
 if-exceeding {
 bandwidth-limit 100m;
```

```
 burst-size-limit 150m;
 }
 then discard;
}
```

Creating a policer for each customer is clearly not a scalable solution, however. As an alternative, you can create prefix lists that group classes of customers and then create policers for each prefix list. For example, you could create prefix lists such as **Class-A-Customer-Prefixes**, **Class-B-Customer-Prefixes**, and **Class-C-Customer-Prefixes** (at the **[edit policy-options]** hierarchy level) and create the following corresponding policers:

```
firewall {
 policer Class-A {
 if-exceeding {
 bandwidth-limit 100m;
 burst-size-limit 150m;
 }
 then discard;
 }
 policer Class-B {
 if-exceeding {
 bandwidth-limit 75m;
 burst-size-limit 100m;
 }
 then discard;
 }
 policer Class-C {
 if-exceeding {
 bandwidth-limit 50m;
 burst-size-limit 75m;
 }
 then discard;
 }
}
```

You must create filter terms that specify the prefix lists in their **from** statements and the corresponding policers in their **then** statements similar to the following:

```
firewall
 family inet {
 filter Class-A-Customers {
 term term-1 {
 from {
 destination-prefix-list {
 Class-A-Customer-Prefixes;
 }
 }
 then policer Class-A;
 }
 }
 filter Class-B-Customers {
 term term-1 {
 from {
 destination-prefix-list {
 Class-B-Customer-Prefixes;
 }
 }
 then policer Class-B;
 }
 }
 }
```

```

 }
 }
 then policer Class-B;
}
}
filter Class-C-Customers {
 term term-1 {
 from {
 destination-prefix-list {
 Class-C-Customer-Prefixes;
 }
 }
 then policer Class-C;
 }
}
}

```

Here are the steps to create this firewall configuration:

1. Create the first policer:

```

[edit firewall]
user@switch# set policer Class-A if-exceeding bandwidth-limit 100m burst-size-limit 150m
user@switch# set policer Class-A then discard

```

2. Create the second policer:

```

[edit firewall]
user@switch# set policer Class-B if-exceeding bandwidth-limit 75m burst-size-limit 100m
user@switch# set policer Class-B then discard

```

3. Create the third policer:

```

[edit firewall]
user@switch# set policer Class-C if-exceeding bandwidth-limit 50m burst-size-limit 75m
user@switch# set policer Class-C then discard

```

4. Create a filter for class A customers:

```

[edit firewall]
user@switch# edit family inet filter Class-A-Customers

```

5. Configure the filter to send packets matching the **Class-A-Customer-Prefixes** prefix list to the **Class-A** policer:

```

[edit firewall family inet filter Class-A-Customers]
user@switch# set term term-1 from source-prefix-list Class-A-Customers
user@switch# set term term-1 then policer Class-A

```

6. Create a filter for class B customers:

```

[edit firewall]
user@switch# edit family inet filter Class-B-Customers

```

7. Configure the filter to send packets matching the **Class-B-Customer-Prefixes** prefix list to the **Class-B** policer:

```

[edit firewall family inet filter Class-B-Customers]
user@switch# set term term-1 from source-prefix-list Class-B-Customers
user@switch# set term term-1 then policer Class-B

```

8. Create a filter for class C customers:

```

[edit firewall]
user@switch# edit family inet filter Class-C-Customers

```

9. Configure the filter to send packets matching the **Class-C-Customer-Prefixes** prefix list to the **Class-C** policer:

```
[edit firewall family inet filter Class-C-Customers]
user@switch# set term term-1 from source-prefix-list Class-C-Customers
user@switch# set term term-1 then policer Class-C
```

10. Apply the filters you created to the appropriate interfaces in the output direction.



**NOTE:** Note that the implicit deny statement in this filter will block traffic from any source that does not match one of the prefix lists. If you want the filter to allow this traffic, you must include an explicit term for this purpose.

#### Related Documentation

- [Overview of Policers on page 61](#)
- [Applying Firewall Filters to Interfaces](#)
- [prefix-list](#)

## Example: Using Policers to Manage Oversubscription

You might want to use a policer when an interface is oversubscribed and you want to control what will happen if congestion occurs. For example, you might have servers connected to a switch as listed in [Table 13 on page 78](#).

**Table 13: Servers Connected to Switch**

| Server Type                | Connection           | IP Address |
|----------------------------|----------------------|------------|
| Network application server | 1-gigabit interface  | 10.0.0.1   |
| Authentication server      | 1-gigabit interface  | 10.0.0.2   |
| Database server            | 10-gigabit interface | 10.0.0.3   |

In this example, users access services provided by the network application server, which requests information from the database server as appropriate. When it receives a request from a user, the network application server first contacts the authentication server to verify the user's credentials. When a user is authenticated and the network application server provides the requested service, all the packets sent from the database server to the application server must transit the 1-Gigabit Ethernet interface connected to the application server twice—once on ingress to the application server and again on egress to the user.

The sequence of events for a user session is as follows:

1. A user connects to the application server and requests a service.
2. The application server requests the user's credentials and relays them to the authentication server.
3. If the authentication server verifies the credentials, the application server initiates the requested service.

4. The application server requests the files necessary to meet the user's request from the database server.
5. The database server sends the requested files to the application server.
6. The application server includes the requested files in its response to the user.

Traffic from the database server to the application server might congest the 1-gigabit interface to which that the application server is connected. This congestion might prevent the server from responding to requests from users and creating new sessions for them. You can use policing to make sure that this does not occur.

To create this firewall configuration, perform the following steps on the database server:

1. Create a policer to drop traffic from the database server to the application server if it exceeds certain limits:

```
[edit firewall]
user@switch# set policer Database-Egress-Policer if-exceeding bandwidth-limit 400
burst-size-limit 500m
user@switch# set policer Database-Egress-Policer then discard
```

2. Create a filter to examine traffic from the database server to the application server:

```
[edit firewall]
user@switch# edit family inet filter Database-Egress-Filter
```

3. Configure the filter to apply the policer to traffic egressing the database server and destined for the application server:

```
[edit firewall family inet filter Database-Egress-Filter]
user@switch# set term term-1 from destination-address 10.0.0.1
user@switch# set term term-1 then policer Database-Egress-Policer
```

4. If required, configure a term to allow traffic from the database server to other destinations (otherwise the traffic will be dropped by the implicit deny statement):

```
[edit firewall family inet filter Database-Egress-Filter]
user@switch# set term term-2 then accept
```

Note that omitting a **from** statement causes the term to match all packets, which is the desired behavior.

5. Install the egress filter as an output filter on the database server interface that is connected the application server:

```
[edit interfaces]
user@switch# set xe-0/0/3 unit 0 family inet filter output Database-Egress-Filter
```

Here is how the final configuration would appear:

```
firewall {
 policer Database-Egress-Policer {
 if-exceeding {
 bandwidth-limit 400;
 burst-size-limit 500m;
 }
 then discard;
 }
 family inet {
 filter Database-Egress-Filter {
 term term-1 {
```

```

 from {
 destination-address {
 10.0.0.1/24;
 }
 }
 then policer Database-Egress-Policer;
}
term term-2 { # If required, include this term so that traffic from the database server
 to other destinations is allowed.
 then accept;
}
}
]

```

**Related Documentation**

- [Overview of Policers on page 61](#)

## Assigning Forwarding Classes and Loss Priority

You can configure firewall filters to assign packet loss priority (PLP) and forwarding classes so that if congestion occurs, the marked packets can be dropped according to the priority you set. The valid match conditions are one or more of the six packet header fields: destination address, source address, IP protocol, source port, destination port, and DSCP. In other words, you can set the forwarding class and the PLP for each packet entering or an interface with a specific destination address, source address, IP protocol, source port, destination port, or DSCP.



**NOTE:** Junos OS assigns forwarding classes and PLP on ingress only. Do not use a filter that assigns forwarding classes or PLP as an egress filter.

When tricolor marking is enabled, a switch supports four PLP designations: **low**, **medium-low**, **medium-high**, and **high**. You can also specify any of the forwarding classes listed in [Table 14 on page 80](#)

**Table 14: Unicast Forwarding Classes**

| Unicast Forwarding Class | For CoS Traffic Type                                               |
|--------------------------|--------------------------------------------------------------------|
| <b>be</b>                | Best-effort traffic                                                |
| <b>no-loss</b>           | Guaranteed delivery for TCP traffic                                |
| <b>fcoe</b>              | Guaranteed delivery for Fibre Channel over Ethernet (FCoE) traffic |
| <b>nc</b>                | Network-control traffic                                            |

To assign forwarding classes in firewall filters:

1. Configure the family address type and filter name:

```
[edit]
```

```
user@switch# edit firewall family ethernet-switching filter ingress-filter
```

2. Configure the terms of the filter as appropriate, including the **forwarding-class** and **loss-priority** action modifiers. For example, each of the following terms in the filter examines various packet header fields and assigns the appropriate forwarding class and packet loss priority:

- The term **corp-traffic** matches all IPv4 packets with a 10.1.1.0/24 source address and assigns the packets to forwarding class **no-loss** with a loss priority of **low**:

```
[edit firewall family ethernet-switching filter ingress-filter]
user@switch# set term corp-traffic from source-address 10.1.1.0/24;
user@switch# set term corp-traffic then forwarding-class no-loss
user@switch# set term corp-traffic then loss-priority low
```

- The term **data-traffic** matches all IPv4 packets with a 10.1.2.0/24 source address and assigns the packets to forwarding class **be** (best effort) with a loss priority of **medium-high**:

```
[edit firewall family ethernet-switching filter ingress-filter]
user@switch# set term data-traffic from source-address 10.1.2.0/24;
user@switch# set term data-traffic then forwarding-class be
user@switch# set term data-traffic then loss-priority medium-high
```

- Because the loss of network-generated packets can jeopardize proper network operation, the delay of these packets is preferable to discarding these packets. The term **network-traffic** assigns the packets with an IP precedence of **net-control** to forwarding class **nc** (network control) with a loss priority of **low**:

```
[edit firewall family ethernet-switching filter ingress-filter]
user@switch# set term network-traffic from precedence net-control
user@switch# set term network-traffic then forwarding-class nc
user@switch# set term network-traffic then loss-priority low
```

- The last term **accept-traffic** matches any packets that did not match on any of the preceding terms and assigns the packets to forwarding class **be** with a loss priority of **high**:

```
[edit firewall family ethernet-switching filter ingress-filter]
user@switch# set term accept-traffic then forwarding-class be
user@switch# set term accept-traffic then loss-priority high
```

3. Apply the filter **ingress-filter** to a port, VLAN, or Layer 3 interface. For information about applying the filter, see “[Configuring Firewall Filters](#)” on page 39. (Assigning forwarding classes and PLP is supported only on ingress filters.)

#### Related Documentation

- [Configuring Firewall Filters on page 39](#)
- [Verifying That Firewall Filters Are Operational on page 50](#)
- [Monitoring Firewall Filter Traffic on page 49](#)
- [Overview of Policers on page 61](#)
- [Understanding CoS Classifiers](#)
- [Understanding CoS Forwarding Classes](#)

## Configuring Color-Blind Egress Policers for Medium-Low PLP

If you use color-blind mode and want to configure an egress policer that marks packets to have medium-low PLP, you must configure a single-rate two-color policer at the **[edit firewall policer *policer-name*]** hierarchy level, because color-blind mode does not support medium-low priority. For example:

1. Specify the name of the policer, the bandwidth limit in bits per second (bps) to control the traffic rate on an interface, and the maximum allowed burst size to control the amount of traffic bursting:

```
[edit]
user@switch# set firewall policer policer-name if-exceeding bandwidth-limit bytes
burst-size-limit bytes
```

2. Specify medium-low loss priority for matching packets:

```
[edit]
user@switch# set firewall policer policer-name then loss-priority medium-low;
```

3. Apply the filter to a port, VLAN, or Layer 3 interface.

### Related Documentation

- [Overview of Policers on page 61](#)
- [Understanding Color-Blind Mode for Single-Rate Tricolor Marking on page 67](#)
- [Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 69](#)
- [Configuring Firewall Filters on page 39](#)
- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82](#)

## Configuring Two-Color and Three-Color Policers to Control Traffic Rates

You can rate-limit traffic by configuring a policer and specifying it as an action modifier for a term in a firewall filter. By default, if you specify the same policer in multiple terms, Junos OS creates a separate policer instance for each term and applies rate limiting separately for each instance. For example, if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, each policer instance enforces a 1-Gbps limit. In this case, the total bandwidth allowed by the filter is 3 Gbps.

You can also configure a policer to be filter-specific, which means that Junos OS creates only one policer instance regardless of how many times the policer is referenced. When you do this, rate limiting is applied in aggregate, so if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, the total bandwidth allowed by the filter is 1 Gbps.



**NOTE:** You can include two-color policer actions on ingress firewall filters only. You can include three-color policer actions on ingress and egress filters.

1. [Configuring Two-Color Policers on page 83](#)
2. [Configuring Three-Color Policers on page 83](#)



3. [Specifying Policers in a Firewall Filter Configuration on page 84](#)
4. [Applying a Firewall Filter That Includes a Policer on page 84](#)

## Configuring Two-Color Policers

To configure a two-color policer:

1. Specify the name of the policer, the bandwidth limit to control the traffic rate on an interface, and the maximum allowed burst size to control the amount of traffic bursting:

```
[edit firewall]
user@switch# set policer policer-name <filter-specific> if-exceeding bandwidth-limit bps
burst-size-limit bytes
```

The policer name can contain letters, numbers, and hyphens (-) and can have as many as 64 characters.

The range for the bandwidth limit is 32000 (32k) through 102,300,000,000 (102300m) bps.

To determine the value for the burst-size limit, multiply the bandwidth of the interface on which the filter is applied by the amount of time to allow a burst of traffic at that bandwidth to occur and divide the result by 8:

**maximum burst size = (interface bandwidth) X (allowable time for burst) / (8 bits/byte)**

The range for the burst-size limit is 1 through 2,147,450,880 bytes.

2. Specify the policer action to discard or assign a loss priority to packets that exceed the rate limits:

```
[edit firewall policer policer-name]
user@switch# set then (discard | loss-priority low | loss-priority high)
```

## Configuring Three-Color Policers

To configure a three-color policer:

1. Specify the name of the policer and (optionally) whether to automatically discard packets with high loss priority (PLP):

```
[edit firewall]
user@switch# set three-color-policer policer-name
user@switch# set three-color-policer policer-name action loss-priority high then discard
```

2. Specify whether the three-color policer should be single-rate or two-rate and whether it should be color-aware or color-blind:

```
[edit firewall three-color-policer policer-name]
user@switch# set (single-rate | two-rate) (color-aware | color-blind)
```

3. For single-rate three-color policers, configure the CIR, CBS, and EBS:

```
[edit firewall three-color-policer policer-name single-rate]
user@switch# set committed-information-rate bps
user@switch# set committed-burst-size bytes
user@switch# set excess-burst-size bytes
```

4. For two-rate three-color policers, configure the CIR, CBS, PIR, and PBS:

```
[edit firewall three-color-policer policer-name single-rate]
user@switch# set committed-information-rate bps
user@switch# set committed-burst-size bytes
```

```

user@switch# set peak-information-rate bps
user@switch# set peak-burst-size bytes

```

## Specifying Policers in a Firewall Filter Configuration

To use a two-color policer, configure a filter term that includes the action **policer**:

```

[edit firewall family family-name]
user@switch# set filter filter-name term name then name

```

For example, the following commands apply a two-color policer to all packets sent from 192.0.2.0/24.

```

[edit firewall family family-name]
user@switch# set filter limit-hosts term term1 from source-address 192.0.2.0/24
user@switch# set filter limit-hosts term term1 then policer policer1

```

To use a three-color policer, configure a filter term that includes the action **three-color-policer**:

```

[edit firewall family name]
user@switch# set filter name term name from match-condition
user@switch# set filter name term name then three-color-policer (single-rate | two-rate) name

```

For example, the following commands apply a single-rate three-color policer to all packets received or sent by interface **ge-0/0/6** (depending on whether the filter is an ingress or egress filter).

```

[edit firewall family name]
user@switch# set filter srTCM term term-one from interface ge-0/0/6
user@switch# set filter srTCM term term-one then three-color-policer single-rate srTCM1-ca

```

You must specify whether the three-color policer is single-rate or two-rate, and this must match the policer itself. Otherwise, the configuration listing includes an error message indicating that the three-color policer you referenced in the filter does not exist.

## Applying a Firewall Filter That Includes a Policer

A firewall filter that includes one or more policer action modifiers must be applied to a port, VLAN, or Layer 3 interface like any other filter. For information about applying firewall filters, see “Configuring Firewall Filters” on page 39.



**NOTE:** You can include two-color policer actions on ingress firewall filters only. You can include three-color policer actions on ingress and egress filters.

### Related Documentation

- [Configuring Firewall Filters on page 39](#)
- [Overview of Policers on page 61](#)
- [Verifying That Two-Color Policers Are Operational on page 85](#)
- [Verifying That Three-Color Policers Are Operational on page 84](#)
- [Configuring Color-Blind Egress Policers for Medium-Low PLP on page 82](#)

## Verifying That Three-Color Policers Are Operational

**Purpose** Verify that three-color policers in firewall filter configurations are working properly.

**Action** Use the following operational mode commands to verify that a three-color policer is working properly:

- `show class-of-service forwarding-table classifiers`
- `show interfaces interface-name extensive`
- `show interfaces queue interface-name`

**Related Documentation**

- [Overview of Policers on page 61](#)
- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82](#)

## Verifying That Two-Color Policers Are Operational

**Purpose** Verify that two-color policers in firewall filter configurations are working properly.

**Action** Use the `show firewall policer` operational mode command to verify that the policers are working properly:

```
user@switch> show firewall policer
Filter: egress-vlan-watch-employee
Filter: ingress-port-filter
Filter: ingress-port-limit-tcp-icmp
Policers:
Name Packets
icmp-connection-policer 10
tcp-connection-policer 539
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```

**Meaning** The `show firewall policer` command displays the names of all firewall filters and policers that are configured. For each policer that is specified in a filter configuration, the output field shows the current packet count for all packets that exceed the specified rate limits.

**Related Documentation**

- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82](#)
- [Configuring Firewall Filters on page 39](#)
- [Monitoring Firewall Filter Traffic on page 49](#)

## Troubleshooting Policer Configuration

- [Incomplete Count of Packet Drops on page 86](#)
- [Counter Reset When Editing Filter on page 86](#)
- [Invalid Statistics for Policer on page 86](#)
- [Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured on page 86](#)

- [Filter-Specific Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured on page 87](#)
- [Policers Can Limit Egress Filters on page 88](#)

## Incomplete Count of Packet Drops

**Problem**    **Description:** Under certain circumstances, Junos OS might display a misleading number of packets dropped by an ingress policer.

If packets are dropped because of ingress admission control, policer statistics might not show the number of packet drops you would expect by calculating the difference between ingress and egress packet counts. This might happen if you apply an ingress policer to multiple interfaces, and the aggregate ingress rate of those interfaces exceeds the line rate of a common egress interface. In this case, packets might be dropped from the ingress buffer. These drops are not included in the count of packets dropped by the policer, which causes policer statistics to underreport the total number of drops.

**Solution**    This is expected behavior.

## Counter Reset When Editing Filter

**Problem**    **Description:** If you edit a firewall filter term, the value of any counter associated with any term in the same filter is set to 0, including the implicit counter for any policer referenced by the filter. Consider the following examples:

- Assume that your filter has **term1**, **term2**, and **term3**, and each term has a counter that has already counted matching packets. If you edit any of the terms in any way, the counters for all the terms are reset to 0.
- Assume that your filter has **term1** and **term2**. Also assume that **term2** has a **policer** action modifier and the implicit counter of the policer has already counted 1000 matching packets. If you edit **term1** or **term2** in any way, the counter for the policer referenced by **term2** is reset to 0.

**Solution**    This is expected behavior.

## Invalid Statistics for Policer

**Problem**    **Description:** If you apply a single-rate two-color policer in more than 128 terms in a firewall filter, the output of the **show firewall** command displays incorrect data for the policer.

**Solution**    This is expected behavior.

## Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured

**Problem**    **Description:** If you configure a policer to rate-limit throughput and apply it on egress to multiple interfaces on a QFX3500 switch or Node, the measured aggregate policed rate might be twice the configured rate, depending on which interfaces you apply the policer

to. The doubling of the policed rate occurs if you apply a policer to multiple interfaces and *both* of the following are true:

- There is at least one policed interface in the range xe-0/0/0 to xe-0/0/23 or the range xe-0/1/1 to xe-0/1/7.
- There is at least one policed interface in the range xe-0/0/24 to xe-0/0/47 or the range xe-0/1/8 to xe-0/1/15.

For example, if you configure a policer to rate-limit traffic at 1 Gbps and apply the policer (by using a firewall filter) to xe-0/0/0 and xe-0/0/24 in the output direction, each interface is rate-limited at 1 Gbps, for a total allowed throughput of 2 Gbps. The same behavior occurs if you apply the policer to xe-0/1/1 and xe-0/0/24—each interface is rate-limited at 1 Gbps.

If you apply the same policer on egress to multiple interfaces in these groups, each *group* is rate-limited at 1 Gbps. For example, if you apply the policer to xe-0/0/0 through xe-0/0/4 (five interfaces) and xe-0/0/24 through xe-0/0/33 (ten interfaces), each group is rate-limited at 1 Gbps, for a total allowed throughput of 2 Gbps.

Here is another example: If you apply the policer to xe-0/0/0 through xe-0/0/4 and xe-0/1/1 through xe-0/1/5 (a total of ten interfaces), that group is rate-limited at 1 Gbps in aggregate. If you also apply the policer to xe-0/0/24, that one interface is rate-limited at 1 Gbps while the other ten are still rate-limited at 1 Gbps in aggregate.

Interfaces xe-0/1/1 through xe-0/1/15 are physically located on the QSFP+ uplink ports, according to the following scheme:

- xe-0/1/1 through xe-0/1/3 are on Q0.
- xe-0/1/4 through xe-0/1/7 are on Q1.
- xe-0/1/8 through xe-0/1/11 are on Q2.
- xe-0/1/12 through xe-0/1/15 are on Q3.

The doubling of the policed rate occurs only if the policer is applied in the output direction. If you configure a policer as described above but apply it in the input direction, the total allowed throughput for all interfaces is 1 Gbps.

**Solution** This is expected behavior.

## Filter-Specific Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured

**Problem Description:** You can configure policers to be filter-specific, which means that Junos OS creates only one policer instance regardless of how many times the policer is referenced. When you do this, rate limiting is applied in aggregate, so if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, the total bandwidth allowed by the filter is 1 Gbps. However, the behavior of a filter-specific policer is affected by how the firewall filter terms that reference the policer are stored in ternary content addressable memory (TCAM). If you create a filter-specific policer and reference it in multiple firewall filter terms, the policer allows more traffic than expected

if the terms are stored in different TCAM slices. For example, if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms that are stored in three separate memory slices, the total bandwidth allowed by the filter is 3 Gbps, not 1 Gbps.

**Solution** To prevent this unexpected behavior, use the information about TCAM slices presented in [“Planning the Number of Firewall Filters to Create” on page 34](#) to organize your configuration file so that all the firewall filter terms that reference a given filter-specific policer are stored in the same TCAM slice.

## Policers Can Limit Egress Filters

**Problem** **Description:** The number of egress policers that you configure can affect the total number of allowed egress firewall filters. Every policer has two implicit counters that consume two entries in a 1024-entry TCAM that is used for counters, including counters that are configured as action modifiers in firewall filter terms. (Policers consume two entries because one is used for green packets and one is used for nongreen packets regardless of policer type.) If the TCAM becomes full, you cannot commit any more egress firewall filters that have terms with counters. For example, if you configure and commit 512 egress policers (two-color, three-color, or a combination of both policer types), all of the memory entries for counters are used up. If later in your configuration file you insert additional egress firewall filters with terms that also include counters, *none* of the terms in those filters are committed because there is no available memory space for the counters. Here are some additional examples:

- Assume that you configure egress filters that include a total of 512 policers and no counters. Later in your configuration file you include another egress filter with 10 terms, 1 of which has a counter action modifier. None of the terms in this filter are committed because there is not enough TCAM space for the counter.
- Assume that you configure egress filters that include a total of 500 policers, so 1000 TCAM entries are occupied. Later in your configuration file you include the following two egress filters:
  - Filter A with 20 terms and 20 counters. All the terms in this filter are committed because there is enough TCAM space for all the counters.
  - Filter B comes after Filter A and has five terms and five counters. *None* of the terms in this filter are committed because there is not enough memory space for *all* the counters. (Five TCAM entries are required but only four are available.)

**Solution** You can prevent this problem by ensuring that egress firewall filter terms with counter actions are placed earlier in your configuration file than terms that include policers. In this circumstance, Junos OS commits policers even if there is not enough TCAM space for the implicit counters. For example, assume the following:

- You have 1024 egress firewall filter terms with counter actions.

- Later in your configuration file you have an egress filter with 10 terms. None of the terms have counters but one has a policer action modifier.

You can successfully commit the filter with 10 terms even though there is not enough TCAM space for the implicit counters of the policer. The policer is committed without the counters.





## PART 3

# Media Access Control Security (MACsec)

- [Using MACsec on page 93](#)



## CHAPTER 3

# Using MACsec

- [Understanding Media Access Control Security \(MACsec\) on page 93](#)
- [Configuring Media Access Control Security \(MACsec\) on page 99](#)

### Understanding Media Access Control Security (MACsec)

Media Access Control Security (MACsec) is an industry-standard security technology that provides secure communication for all traffic on Ethernet links. MACsec provides point-to-point security on Ethernet links between directly connected nodes and is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks. MACsec is standardized in IEEE 802.1AE.

MACsec allows you to secure an Ethernet link for almost all traffic, including frames from the Link Layer Discovery Protocol (LLDP), Link Aggregation Control Protocol (LACP), Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), and other protocols that are not typically secured on an Ethernet link because of limitations with other security solutions. MACsec can be used in combination with other security protocols such as IP Security (IPsec) and Secure Sockets Layer (SSL) to provide end-to-end network security.

This topic contains the following sections:

- [How MACsec Works on page 94](#)
- [Understanding Connectivity Associations and Secure Channels on page 94](#)
- [Understanding MACsec Security Modes on page 95](#)
- [Understanding the Requirements to Enable MACsec on a Switch-to-Host Link on page 97](#)
- [Understanding MACsec Hardware Requirements for EX Series and QFX Series Switches on page 97](#)
- [Understanding MACsec Software Requirements for EX Series and QFX Series Switches on page 98](#)
- [Understanding the MACsec Feature License Requirement on page 99](#)
- [MACsec Limitations on page 99](#)

## How MACsec Works

MACsec provides industry-standard security through the use of secured point-to-point Ethernet links. The point-to-point links are secured after matching security keys—a user-configured pre-shared key when you enable MACsec using static connectivity association key (CAK) security mode, a user-configured static secure association key when you enable MACsec using static secure association key (SAK) security mode, or a dynamic key included as part of the AAA handshake with the RADIUS server when you enable MACsec using dynamic security mode—are exchanged and verified between the interfaces at each end of the point-to-point Ethernet link. Other user-configurable parameters, such as MAC address or port, must also match on the interfaces on each side of the link to enable MACsec. See [“Configuring Media Access Control Security \(MACsec\)” on page 99](#).

Once MACsec is enabled on a point-to-point Ethernet link, all traffic traversing the link is MACsec-secured through the use of data integrity checks and, if configured, encryption.

The data integrity checks verify the integrity of the data. MACsec appends an 8-byte header and a 16-byte tail to all Ethernet frames traversing the MACsec-secured point-to-point Ethernet link, and the header and tail are checked by the receiving interface to ensure that the data was not compromised while traversing the link. If the data integrity check detects anything irregular about the traffic, the traffic is dropped.

MACsec can also be used to encrypt all traffic on the Ethernet link. The encryption used by MACsec ensures that the data in the Ethernet frame cannot be viewed by anybody monitoring traffic on the link. MACsec encryption is optional and user-configurable; you can enable MACsec to ensure the data integrity checks are performed while still sending unencrypted data “in the clear” over the MACsec-secured link, if desired.

MACsec is configured on point-to-point Ethernet links between MACsec-capable interfaces. If you want to enable MACsec on multiple Ethernet links, you must configure MACsec individually on each point-to-point Ethernet link.

## Understanding Connectivity Associations and Secure Channels

MACsec is configured in connectivity associations. MACsec is enabled when a connectivity association is assigned to an interface.

When you are configuring MACsec using static secure association key (SAK) security mode, you must configure secure channels within a connectivity association. The secure channels are responsible for transmitting and receiving data on the MACsec-enabled link, and also responsible for transmitting SAKs across the link to enable and maintain MACsec. A single secure channel is uni-directional—it can only be used to apply MACsec to inbound or outbound traffic. A typical connectivity association when MACsec is enabled using SAK security mode contains two secure channels—one secure channel for inbound traffic and another secure channel for outbound traffic.

When you enable MACsec using static CAK or dynamic security mode, you have to create and configure a connectivity association. Two secure channels—one secure channel for inbound traffic and another secure channel for outbound traffic—are automatically created. The automatically-created secure channels do not have any user-configurable

parameters; all configuration is done in the connectivity association outside of the secure channels.

## Understanding MACsec Security Modes

### Understanding Static Connectivity Association Key Security Mode (Recommended Security Mode for Switch-to-Switch Links)

---

When you enable MACsec using static connectivity association key (CAK) security mode, two security keys—a connectivity association key (CAK) that secures control plane traffic and a randomly-generated secure association key (SAK) that secures data plane traffic—are used to secure the point-to-point Ethernet link. Both keys are regularly exchanged between both devices on each end of the point-to-point Ethernet link to ensure link security.

You initially establish a MACsec-secured link using a pre-shared key when you are using static CAK security mode to enable MACsec. A pre-shared key includes a connectivity association name (CKN) and its own connectivity association key (CAK). The CKN and CAK are configured by the user in the connectivity association and must match on both ends of the link to initially enable MACsec.

Once matching pre-shared keys are successfully exchanged, the MACsec Key Agreement (MKA) protocol is enabled. The MKA protocol is responsible for maintaining MACsec on the link, and decides which switch on the point-to-point link becomes the key server. The key server then creates an SAK that is shared with the switch at the other end of the point-to-point link only, and that SAK is used to secure all data traffic traversing the link. The key server will continue to periodically create and share a randomly-created SAK over the point-to-point link for as long as MACsec is enabled.

You enable MACsec using static CAK security mode by configuring a connectivity association on both ends of the link. All configuration is done within the connectivity association but outside of the secure channel. Two secure channels—one for inbound traffic and one for outbound traffic—are automatically created when using static CAK security mode. The automatically-created secure channels do not have any user-configurable parameters that cannot already be configured in the connectivity association.

We recommend enabling MACsec on switch-to-switch links using static CAK security mode. Static CAK security mode ensures security by frequently refreshing to a new random security key and by only sharing the security key between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available when you enable MACsec using static CAK security mode.

See [“Configuring Media Access Control Security \(MACsec\)” on page 99](#) for step-by-step instructions on enabling MACsec using static CAK security mode.

### Understanding Dynamic Secure Association Key Security Mode (Switch-to-Host Links)

---

Dynamic secure association key security mode is used to enable MACsec on a switch-to-host link.

To enable MACsec on a link connecting an endpoint device—such as a server, phone, or personal computer—to a switch, the endpoint device must support MACsec and must be running software that allows it to enable a MACsec-secured connection. When configuring MACsec on a switch-to-host link, the MACsec Key Agreement (MKA) keys, which are included as part of 802.1X authentication, are retrieved from a RADIUS server as part of the AAA handshake. A master key is passed from the RADIUS server to the switch and from the RADIUS server to the host in independent authentication transactions. The master key is then passed between the switch and the host to create a MACsec-secured connection.

A secure association using dynamic secure association security mode must be configured on the switch's Ethernet interface that connects to the host in order for the switch to create a MACsec-secured connection after receiving the MKA keys from the RADIUS server.

The RADIUS server must be using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) in order to support MACsec. The RADIUS servers that support other widely-used authentication frameworks, such as password-only or md5, cannot be used to support MACsec. In order to enable MACsec on a switch to secure a connection to a host, you must be using 802.1X authentication on the RADIUS server. MACsec must be configured into dynamic mode. MACsec is still enabled using connectivity associations when enabled on a switch-to-host link, as it is on a switch-to-switch link.

### **Understanding Static Secure Association Key Security Mode (Supported for Switch-to-Switch Links)**

---

When you enable MACsec using static secure association key (SAK) security mode, one of up to two manually configured SAKs is used to secure data traffic on the point-to-point Ethernet link. All SAK names and values are configured by the user; there is no key server or other tool that creates SAKs. Security is maintained on the point-to-point Ethernet link by periodically rotating between the two security keys. Each security key name and value must have a corresponding matching value on the interface at the other end of the point-to-point Ethernet link to maintain MACsec on the link.

You configure SAKs within secure channels when you enable MACsec using static SAK security mode. You configure secure channels within connectivity associations. A typical connectivity association for MACsec using static SAK security mode contains two secure channels—one for inbound traffic and one for outbound traffic—that have each been configured with two manually-configured SAKs. You must attach the connectivity association with the secure channel configurations to an interface to enable MACsec using static SAK security mode.

We recommend enabling MACsec using static CAK security mode. You should only use static SAK security mode if you have a compelling reason to use it instead of static CAK security mode.

See [“Configuring Media Access Control Security \(MACsec\)” on page 99](#) for step-by-step instructions on enabling MACsec using SAKs.

## Understanding the Requirements to Enable MACsec on a Switch-to-Host Link

When configuring MACsec on a switch-to-host link, the MACsec Key Agreement (MKA) keys, which are included as part of 802.1X authentication, are retrieved from a RADIUS server as part of the AAA handshake. A master key is passed from the RADIUS server to the switch and from the RADIUS server to the host in independent authentication transactions. The master key is then passed between the switch and the host to create a MACsec-secured connection.

The following requirements must be met in order to enable MACsec on a link connecting a host device to a switch.

The host device:

- must support MACsec and must be running software that allows it to enable a MACsec-secured connection with the switch.

The switch:

- must be an EX4200, EX4300, or EX4550 switch running Junos OS Release 14.1X53-D10 or later
- must be configured into dynamic secure association key security mode.
- must be using 802.1X authentication to communicate with the RADIUS server.

The RADIUS server:

- must be using the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication framework.



**NOTE:** RADIUS servers that support other widely-used authentication frameworks, such as password-only or md5, cannot be used to support MACsec.

- must be using 802.1X authentication.
- can be multiple hops from the switch and the host device.

## Understanding MACsec Hardware Requirements for EX Series and QFX Series Switches

MACsec is currently supported on the following EX Series and QFX Series switch interfaces:

- The uplink port connections on the SFP+ MACsec uplink module that can be installed on EX4200 series switches.
- All access and uplink ports on EX4300 switches.
- All EX4550 optical interfaces that use the LC connection type. See *Pluggable Transceivers Supported on EX4550 Switches*.

- All twenty-four fixed 1GbE SFP/10GbE SFP+ interfaces on an EX4600 switch and all interfaces that support the copper Gigabit Interface Converter (GBIC).
- All eight SFP+ interfaces on the EX4600-EM-8F expansion module, when installed in an EX4600 or QFX5100-24Q switch.

MACsec can be configured on supported switch interfaces when those switches are configured in a Virtual Chassis or Virtual Chassis Fabric (VCF), including when MACsec-supported interfaces are on member switches in a mixed Virtual Chassis or VCF that includes switch interfaces that do not support MACsec. MACsec, however, cannot be enabled on Virtual Chassis ports (VCPs) to secure traffic travelling between member switches in a Virtual Chassis or VCF.

## Understanding MACsec Software Requirements for EX Series and QFX Series Switches

MACsec was initially released on EX4200, EX4300, and EX4550 switches in Junos OS Release 13.2X50-D15.

MACsec support for dynamic security mode, which allows MACsec to be configured on switch-to-host links, for EX4200, EX4300, and EX4550 switches was introduced in Junos OS Release 14.1X53-D10.

MACsec support for EX4600 switches and QFX5100-24Q switches was introduced in Junos OS Release 14.1X53-D15. The EX4600 and QFX5100-24Q switches supports MACsec on switch-to-switch links only.

The switches on each end of a MACsec-secured switch-to-switch link must either both be using Junos OS Release 14.1X53-D10 or later, or must both be using an earlier version of Junos, in order to establish a MACsec-secured connection when using static CAK security mode.

You must download the controlled version of your Junos OS software to enable MACsec. MACsec software support is not available in the domestic version of your Junos OS software. The controlled version of Junos OS software includes all features and functionality available in the domestic version of Junos OS, while also supporting MACsec. The domestic version of Junos OS software is shipped on all switches that support MACsec, so you must download and install a controlled version of Junos OS software for your switch before you can enable MACsec.

The controlled version of Junos OS software contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of the controlled version of Junos OS software is strictly controlled under United States export laws. The export, import, and use of the controlled version of Junos OS software is also subject to controls imposed under the laws of other countries. If you have questions about acquiring the controlled version of your Junos OS software, contact Juniper Networks Trade Compliance group at [compliance\\_helpdesk@juniper.net](mailto:compliance_helpdesk@juniper.net).

The process for installing a controlled version of Junos OS software on your switch is identical to installing the domestic version. See *Downloading Software Packages from Juniper Networks*.



## Understanding the MACsec Feature License Requirement

A feature license is required to configure MACsec on a switch.

To purchase a feature license for MACsec, contact your Juniper Networks sales representative (<http://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper sales representative will provide you with a feature license file and a license key. You will be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the **show chassis hardware** command.

The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on your switches cannot be purchased to enable MACsec.

## MACsec Limitations

All types of Spanning Tree Protocol frames cannot currently be encrypted using MACsec.

### Related Documentation

- [Configuring Media Access Control Security \(MACsec\) on page 99](#)

---

## Configuring Media Access Control Security (MACsec)

Media Access Control Security (MACsec) is an industry-standard security technology that provides secure communication for almost all types of traffic on Ethernet links. MACsec provides point-to-point security on Ethernet links between directly-connected nodes and is capable of identifying and preventing most security threats, including denial of service, intrusion, man-in-the-middle, masquerading, passive wiretapping, and playback attacks. MACsec is standardized in IEEE 802.1AE.

You can configure MACsec to secure point-to-point Ethernet links connecting EX Series or QFX Series switches, or on Ethernet links connecting a switch to a host device such as a PC, phone, or server. Each point-to-point Ethernet link that you want to secure using MACsec must be configured independently. You can enable MACsec on switch-to-switch links using static secure association key (SAK) security mode or static connectivity association key (CAK) security mode. Both processes are provided in this document.



**BEST PRACTICE:** We recommend enabling MACsec using static CAK security mode on switch-to-switch links. Static CAK security mode ensures security by frequently refreshing to a new random secure association key (SAK) and by only sharing the SAK between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available for MACsec-secured switch-to-switch connections that are enabled using static CAK security mode.

The configuration steps for both processes are provided in this document.

- [Acquiring and Downloading the Junos OS Software on page 100](#)
- [Acquiring and Downloading the MACsec Feature License on page 101](#)
- [Configuring the PIC Mode of the MACsec-capable Interfaces \(EX4200 switches only\) on page 102](#)
- [Configuring MACsec Using Static Connectivity Association Key Security Mode \(Recommended for Enabling MACsec on Switch-to-Switch Links\) on page 103](#)
- [Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link on page 107](#)
- [Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link on page 111](#)

## Acquiring and Downloading the Junos OS Software

MACsec was initially released on EX Series switches in Junos OS Release 13.2X50-D15. MACsec was released on EX4600 and QFX5100-24Q switches in Junos OS Release 14.1X53-D15. The switches on each end of a MACsec-secured switch-to-switch link must either both be using Junos OS Release 14.1X51-D10 or later, or must both be using an earlier version of Junos, in order to establish a MACsec-secured connection when using static CAK security mode.

You must download the controlled version of your Junos OS software to enable MACsec. MACsec software support is not available in the domestic version of your Junos OS software. The controlled version of Junos OS software includes all features and functionality available in the domestic version of Junos OS, while also supporting MACsec. The domestic version of Junos OS software is shipped on all EX Series and QFX Series switches, so you must download and install a controlled version of Junos OS software on your switch before you can enable MACsec.

You can identify whether a software package is the controlled or domestic version of Junos OS by viewing the package name. A software package for a controlled version of Junos OS is named using the following format:

***package-name-m.nZx.y-controlled-signed.tgz***

A software package for a domestic version of Junos OS is named using the following format:

***package-name-m.nZx.y-domestic-signed.tgz***

If you are unsure which version of Junos OS is running on your switch, enter the **show version** command. If the "JUNOS Crypto Software Suite" description appears in the output, you are running the controlled version of Junos OS.

The controlled version of Junos OS software contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of the controlled version of Junos OS software is strictly controlled under United States export laws. The export, import, and use of the controlled version of Junos OS software is also subject to

controls imposed under the laws of other countries. If you have questions about acquiring the controlled version of your Junos OS software, contact Juniper Networks Trade Compliance group at [compliance\\_helpdesk@juniper.net](mailto:compliance_helpdesk@juniper.net).

The process for installing the controlled version of Junos OS software on your switch is identical to installing the domestic version of Junos OS software. You must enter the **request system software add** statement to download the Junos OS image, and the **request system reboot** statement to reboot the switch to complete the upgrade procedure. See *Downloading Software Packages from Juniper Networks*, *Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure)*, and *Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)* for detailed information about acquiring and installing Junos OS software images for your switches.

## Acquiring and Downloading the MACsec Feature License

A feature license is required to configure MACsec on an EX Series or a QFX Series switch.

The MACsec feature license is an independent feature license; the enhanced feature licenses (EFLs) or advanced feature licenses (AFLs) that must be purchased to enable some features on EX Series or QFX Series switches cannot be purchased to enable MACsec.

To purchase a software license for MACsec, contact your Juniper Networks sales representative (<http://www.juniper.net/us/en/contact-us/sales-offices>). The Juniper sales representative will provide you with a feature license file and a license key. You will be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the **show chassis hardware** command.

For a Virtual Chassis deployment, two MACsec license keys are recommended for redundancy—one for the device in the master role and the other for the device in the backup role.

To add one or more new MACsec license keys on the switch, follow this procedure:

1. Add the license key or keys:
  - To add one or more license keys from a file or URL, specify the filename of the file or the URL where the key is located:  

```
user@switch> request system license add filename |url
```
  - To add a license key from the terminal:  

```
user@switch> request system license add terminal
```
2. When prompted, enter the license key, separating multiple license keys with a blank line.

If the license key you enter is invalid, an error appears in the CLI output when you press Ctrl+d to exit the license entry mode.

A MACsec feature license is installed and maintained like any other switch license. See *Managing Licenses for the EX Series Switch (CLI Procedure)* or *Adding New Licenses (CLI Procedure)* for more detailed information on configuring and managing your MACsec software license.

## Configuring the PIC Mode of the MACsec-capable Interfaces (EX4200 switches only)

To configure MACsec on an EX4200 switch, you must install the SFP+ MACsec uplink module. The interfaces on the SFP+ MACsec uplink module are the only MACsec-capable interfaces available for EX4200 switches. All four ports on the uplink module are MACsec-capable.

The SFP+ MACsec uplink module provides two ports for 10-gigabit small form-factor pluggable (SFP+) transceivers when configured to operate in 10-gigabit mode or four ports for 1-gigabit small form-factor pluggable (SFP) transceivers when configured to operate in 1-gigabit mode.

The PIC mode is set to **10g**, by default. You only need to perform this procedure if you want to operate your uplink in 1-gigabit mode, or if you previously set the uplink module to 1-gigabit mode and would like to return it to 10-gigabit mode.

To configure the PIC mode:

```
[edit chassis]
```

```
user@switch# set fpc fpc-slot-number pic 1 sfpplus pic-mode (1g | 10g)
```

where *fpc-slot-number* is the FPC slot number, *pic-slot-number* is the PIC slot number, and the **[1g | 10g]** option configures the MACsec capability of the four SFP+ ports on the MACsec uplink module.

The *fpc-slot-number* is always 0 on standalone EX4200 switches, and is the member ID of the member switch in an EX4200 Virtual Chassis.

The PIC slot number is always 1 for the uplink module port slot on an EX4200 switch, so **pic 1** is always the specified PIC slot number.

The PIC mode is set to **10g** by default. When the PIC mode is set to **10g**, uplink ports 0 and 2 on the MACsec uplink module support MACsec at 10-Gbps speeds. Ports 1 and 3 cannot be used to send any traffic.

When the PIC mode is set to **1g**, all four SFP+ ports on the MACsec uplink module support MACsec at 1-Gbps speeds.

## Configuring MACsec Using Static Connectivity Association Key Security Mode (Recommended for Enabling MACsec on Switch-to-Switch Links)

You can enable MACsec using static connectivity association key (CAK) security mode or static secure association keys (SAK) security mode on a point-to-point Ethernet link connecting switches. This procedure shows you how to configure MACsec using static CAK security mode.



**BEST PRACTICE:** We recommend enabling MACsec using static CAK security mode on switch-to-switch links. Static CAK security mode ensures security by frequently refreshing to a new random secure association key (SAK) and by only sharing the SAK between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available for MACsec-secured switch-to-switch connections that are enabled using static CAK security mode.

When you enable MACsec using static CAK security mode, a pre-shared key is exchanged between the switches on each end of the point-to-point Ethernet link. The pre-shared key includes a connectivity association name (CKN) and a connectivity association key (CAK). The CKN and CAK are configured by the user in the connectivity association and must match on both ends of the link to initially enable MACsec.

After the pre-shared keys are exchanged and verified, the MACsec Key Agreement (MKA) protocol, which enables and maintains MACsec on the link, is enabled. The MKA is responsible for selecting one of the two switches on the point-to-point link as the key server. The key server then creates a randomized security key that is shared only with the other device over the MACsec-secured link. The randomized security key enables and maintains MACsec on the point-to-point link. The key server will continue to periodically create and share a randomly-created security key over the point-to-point link for as long as MACsec is enabled.

You enable MACsec using static CAK security mode by configuring a connectivity association on both ends of the link. All configuration is done within the connectivity association but outside of the secure channel. Two secure channels—one for inbound traffic and one for outbound traffic—are automatically created when using static CAK security mode. The automatically-created secure channels do not have any user-configurable parameters that cannot already be configured in the connectivity association.

To configure MACsec using static CAK security mode to secure a switch-to-switch Ethernet link:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name
```

For instance, to create a connectivity association named **ca1**, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca1
```

2. Configure the MACsec security mode as **static-cak** for the connectivity association:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name security-mode
static-cak
```

For instance, to configure the MACsec security mode to **static-cak** on connectivity association **ca1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 security-mode static-cak
```

3. Create the pre-shared key by configuring the connectivity association key name (CKN) and connectivity association key (CAK):

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name pre-shared-key
ckn hexadecimal-number
user@switch# set connectivity-association connectivity-association-name pre-shared-key
cak hexadecimal-number
```

A pre-shared key is exchanged between directly-connected links to establish a MACsec-secure link. The pre-shared-key includes the CKN and the CAK. The CKN is a 64-digit hexadecimal number and the CAK is a 32-digit hexadecimal number. The CKN and the CAK must match on both ends of a link to create a MACsec-secured link.



**NOTE:** To maximize security, we recommend configuring all 64 digits of a CKN and all 32 digits of a CAK.

If you do not configure all 64 digits of a CKN or all 32 digits of a CAK, however, all remaining digits will be auto-configured to 0.

After the pre-shared keys are successfully exchanged and verified by both ends of the link, the MACsec Key Agreement (MKA) protocol is enabled and manages the secure link. The MKA protocol then elects one of the two directly-connected switches as the key server. The key server then shares a random security with the other device over the MACsec-secure point-to-point link. The key server will continue to periodically create and share a random security key with the other device over the MACsec-secured point-to-point link as long as MACsec is enabled.

To configure a CKN of **37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311** and CAK of **228ef255aa23ff6729ee664acb66e91f** on connectivity association **ca1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 pre-shared-key ckn
37c9c2c45ddd012aa5bc8ef284aa23ff6729ee2e4acb66e91fe34ba2cd9fe311
user@switch# set connectivity-association ca1 pre-shared-key cak
228ef255aa23ff6729ee664acb66e91f
```



**NOTE:** MACsec is not enabled until a connectivity association is attached to an interface. See the final step of this procedure to attach a connectivity association to an interface.

4. (Required on switches when connecting to EX4300 switches only) Enable SCI tagging:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set include-sci
```

You must enable SCI tagging on a switch that is enabling MACsec on an Ethernet link connecting to an EX4300 switch.

SCI tags are automatically appended to packets leaving a MACsec-enabled interface on an EX4300 switch. This option is, therefore, not available on EX4300 switches.

You should only use this option when enabling MACsec on a link to an EX4300 switch. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.

5. (Optional) Set the MKA key server priority:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka key-server-priority priority-number
```

Specifies the key server priority used by the MKA protocol to select the key server. The switch with the lower *priority-number* is selected as the key server.

The default *priority-number* is 16.

If the **key-server-priority** is identical on both sides of the point-to-point link, the MKA protocol selects the interface with the lower MAC address as the key server. Therefore, if this statement is not configured in the connectivity associations at each end of a MACsec-secured point-to-point link, the interface with the lower MAC address becomes the key server.

To change the key server priority to 0 to increase the likelihood that the current device is selected as the key server when MACsec is enabled on the interface using connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]
user@switch# set mka key-server-priority 0
```

To change the key server priority to 255 to decrease the likelihood that the current device is selected as the key server in connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]
user@switch# set mka key-server-priority 255
```

6. (Optional) Set the MKA transmit interval:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka transmit-interval interval
```

The MKA transmit interval setting sets the frequency for how often the MKA protocol data unit (PDU) is sent to the directly connected device to maintain MACsec connectivity on the link. A lower *interval* increases bandwidth overhead on the link; a higher *interval* optimizes MKA protocol communication.

The default *interval* is 2000ms. We recommend increasing the interval to 6000 ms in high-traffic load environments. The transmit interval settings must be identical on both ends of the link when MACsec using static CAK security mode is enabled.

For instance, if you wanted to increase the MKA transmit interval to 6000 milliseconds when connectivity association *ca1* is attached to an interface:

```
[edit security macsec connectivity-association ca1]
user@switch# set mka transmit-interval 6000
```

7. (Optional) Disable MACsec encryption:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set no-encryption
```

Encryption is enabled for all traffic entering or leaving the interface when MACsec is enabled using static CAK security mode, by default.

When encryption is disabled, traffic is forwarded across the Ethernet link in clear text. You are able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic sent or received on the link has not been tampered with and does not represent a security threat.

8. (Optional) Set an offset for all packets traversing the link:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set offset (0 | 30 | 50)
```

For instance, if you wanted to set the offset to 30 in the connectivity association named *ca1*:

```
[edit security macsec connectivity-association ca1]
user@switch# set offset 30
```

The default offset is 0. All traffic in the connectivity association is encrypted when encryption is enabled and an **offset** is not set.

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

9. (Optional) Enable replay protection.

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set replay-protect replay-window-size number-of-packets
```

When MACsec is enabled on a link, an ID number is assigned to each packet on the MACsec-secured link.

When replay protection is enabled, the receiving interface checks the ID number of all packets that have traversed the MACsec-secured link. If a packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance,



if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.

Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.

Replay protection should not be enabled in cases where packets are expected to arrive out of order.

You can require that all packets arrive in order by setting the replay window size to 0.

To enable replay protection with a window size of five on connectivity association **ca1**:

```
[edit security macsec connectivity-association ca1]
user@switch# set replay-protect replay-window-size 5
```

10. (Optional) Exclude a protocol from MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set exclude-protocol protocol-name
```

For instance, if you did not want Link Level Discovery Protocol (LLDP) to be secured using MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set exclude-protocol lldp
```

When this option is enabled, MACsec is disabled for all packets of the specified protocol—in this case, LLDP—that are sent or received on the link.

11. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface.

For instance, to assign connectivity association **ca1** to interface **xe-0/0/1**:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca1
```

MACsec using static CAK security mode is not enabled until a connectivity association on the opposite end of the link is also configured, and contains pre-shared keys that match on both ends of the link.

## Configuring MACsec on the Switch Using Dynamic Secure Association Key Security Mode to Secure a Switch-to-Host Link

Before you begin to enable MACsec on a switch-to-host link:

- Configure a RADIUS server. The RADIUS server:
  - must be configured as the user database for 802.1X authentication.
  - must be using the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication framework.

- must have connectivity to the switch and to the host. The RADIUS server can be multiple hops from the switch or the host.

*See Example: Connecting a RADIUS Server for 802.1X to a Switch.*

- Enable MACsec on the host device.

The procedures for enabling MACsec on the host device varies by host device, and is beyond the scope of this document.

To configure MACsec using dynamic security mode to secure a switch-to-host Ethernet link:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

```
[edit security macsec]
```

```
user@switch# set connectivity-association connectivity-association-name
```

For instance, to create a connectivity association named `ca-dynamic1`, enter:

```
[edit security macsec]
```

```
user@switch# set connectivity-association ca-dynamic1
```

2. Configure the MACsec security mode as dynamic for the connectivity association:

```
[edit security macsec]
```

```
user@switch# set connectivity-association connectivity-association-name security-mode dynamic
```

For instance, to configure the MACsec security mode to dynamic on connectivity association `ca-dynamic1`:

```
[edit security macsec]
```

```
user@switch# set connectivity-association ca-dynamic1 security-mode dynamic
```

3. (Optional) Configure the **must-secure** option:

```
[edit security macsec]
```

```
user@switch# set connectivity-association connectivity-association-name mka must-secure
```

When the **must-secure** option is enabled, all traffic that is not MACsec-secured that is received on the interface is dropped.

When the **must-secure** option is disabled, all traffic from devices that support MACsec is MACsec-secured while traffic received from devices that do not support MACsec is forwarded through the network.

The **must-secure** option is particularly useful in scenarios where multiple devices, such as a phone and a PC, are accessing the network through the same Ethernet interface. If one of the devices supports MACsec while the other device does not support MACsec, the device that doesn't support MACsec can continue to send and receive traffic over the network—provided the **must-secure** option is disabled—while traffic to and from the device that supports MACsec is MACsec-secured. In this scenario, traffic to the device that is not MACsec-secured must be VLAN-tagged.

The **must-secure** option is disabled, by default.

4. (Required only if the host device requires SCI tagging) Enable SCI tagging:

```
[edit security macsec connectivity-association connectivity-association-name]
```

```
user@switch# set include-sci
```

You should only use this option when connecting a switch to a host that requires SCI tags. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.

5. (Optional) Set the MKA key server priority:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka key-server-priority priority-number
```

Specifies the key server priority used by the MKA protocol to select the key server. The switch with the lower *priority-number* is selected as the key server.

The default *priority-number* is 16. If the **key-server-priority** is identical on both sides of the point-to-point link, the MKA protocol selects the interface with the lower MAC address as the key server. Therefore, if this statement is not configured in the connectivity associations at each end of a MACsec-secured point-to-point link, the interface with the lower MAC address becomes the key server.

To change the key server priority to 0 to increase the likelihood that the current device is selected as the key server when MACsec is enabled on the interface using connectivity association *ca1*:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set mka key-server-priority 0
```

To change the key server priority to 255 to decrease the likelihood that the current device is selected as the key server in connectivity association *ca-dynamic1*:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set mka key-server-priority 255
```

6. (Optional) Set the MKA transmit interval:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set mka transmit-interval interval
```

The MKA transmit interval setting sets the frequency for how often the MKA protocol data unit (PDU) is sent to the directly connected device to maintain MACsec connectivity on the link. A lower interval increases bandwidth overhead on the link; a higher interval optimizes MKA protocol communication.

The default interval is 2000ms. We recommend increasing the interval to 6000 ms in high-traffic load environments. The transmit interval settings must be identical on both ends of the link.

For instance, if you wanted to increase the MKA transmit interval to 6000 milliseconds when connectivity association *ca-dynamic1* is attached to an interface:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set mka transmit-interval 6000
```

7. (Optional) Disable MACsec encryption:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set no-encryption
```

Encryption is enabled for all traffic entering or leaving the interface when MACsec is enabled using dynamic security mode, by default. When encryption is disabled, traffic is forwarded across the Ethernet link in clear text. You are able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are

run on both ends of the link to ensure the traffic sent or received on the link has not been tampered with and does not represent a security threat.

8. (Optional) Set an offset for all packets traversing the link:

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set offset (0 | 30 | 50)
```

For instance, if you wanted to set the offset to 30 in the connectivity association named ca-dynamic1:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set offset 30
```

The default offset is 0. All traffic in the connectivity association is encrypted when encryption is enabled and an offset is not set.

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

9. (Optional) Enable replay protection.

```
[edit security macsec connectivity-association connectivity-association-name]
user@switch# set replay-protect replay-window-size number-of-packets
```

When MACsec is enabled on a link, an ID number is assigned to each packet on the MACsec-secured link. When replay protection is enabled, the receiving interface checks the ID number of all packets that have traversed the MACsec-secured link. If a packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.

Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.

Replay protection should not be enabled in cases where packets are expected to arrive out of order.

You can require that all packets arrive in order by setting the replay window size to 0.

To enable replay protection with a window size of five on connectivity association ca-dynamic1:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set replay-protect replay-window-size 5
```

10. (Optional) Exclude a protocol from MACsec:

```
[edit security macsec connectivity-association connectivity-association-name]
```

```
user@switch# set exclude-protocol protocol-name
```

For instance, if you did not want Link Level Discovery Protocol (LLDP) to be secured using MACsec:

```
[edit security macsec connectivity-association ca-dynamic1]
user@switch# set exclude-protocol lldp
```

When this option is enabled, MACsec is disabled for all packets of the specified protocol—in this case, LLDP—that are sent or received on the link.

11. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```

Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface. For instance, to assign connectivity association `ca-dynamic1` to interface `xe-0/0/1`:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca-dynamic1
```

## Configuring MACsec Using Static Secure Association Key Security Mode to Secure a Switch-to-Switch Link

When you enable MACsec using static secure association key (SAK) security mode, one of up to two manually configured security keys is used to secure the point-to-point Ethernet link between the switches. All security key names and values are configured by the user; there is no key server or other tool that creates security keys. Security is maintained on the point-to-point Ethernet link by periodically rotating the security keys. Each security key name and value must have a corresponding matching value on the interface at the other end of the point-to-point Ethernet link to maintain MACsec on the link.

You configure static SAKs within secure channels when you are enabling MACsec using static SAK security mode. You configure secure channels within connectivity associations. A typical connectivity association for MACsec using static SAK security mode contains two secure channels—one for inbound traffic and one for outbound traffic—that have each been configured with two static SAKs. You must attach the connectivity association with the secure channel configurations to an interface to enable MACsec using static SAK security mode.

To configure MACsec on a switch-to-switch Ethernet link using static SAK security mode:

1. Create a connectivity association. You can skip this step if you are configuring an existing connectivity association.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name
```

For instance, to create a connectivity association named `ca1`, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca1
```

2. Configure the MACsec security mode as **static-sak** for the connectivity association:

```
[edit security macsec]
```

```
user@switch# set connectivity-association connectivity-association-name security-mode
static-sak
```

For instance, to configure the MACsec security mode to **static-sak** on connectivity association **ca1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 security-mode static-sak
```

3. Create a secure channel within the connectivity association. You can skip this step if you are configuring an existing secure channel.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name
```

For instance, to create secure channel **sc1** in connectivity association **ca1**, enter:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1
```

4. Define the security associations and the static SAKs for the secure channel:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name security-association number key key-string
```

where the **security-association number** is a number between 0 and 3, and the **key-string** is a 32-digit key defined statically by the network administrator.

The key string is a 32-digit hexadecimal number. The key string and the security association must match on both sides of an Ethernet connection to secure traffic using MACsec.

A secure channel must have at least two security associations with unique key strings. MACsec uses a security associations to establish a secure communications link, and periodically rotates to a new security association to keep the link secure. MACsec, therefore, must have at least one backup security association and key at all times.

To create one secure channel with two security associations and keys, for example:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 security-association 0 key
d183c4002fa6fe3d2d9a852c20ab8412
user@switch# set connectivity-association ca1 secure-channel sc1 security-association 1 key
b976c7494ab6fe2f2d4c432a90fd90a8
```

5. Specify whether the secure channel should be applied to traffic entering or leaving the switch:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name direction [inbound | outbound]
```

where **inbound** applies the secure channel to traffic entering the switch, and **outbound** applies the secure channel to traffic leaving the switch.



**NOTE:** A secure channel can only be applied to traffic entering (inbound) or leaving (outbound) an interface on the switch.

If you need to configure MACsec using SAKs on inbound and outbound traffic on the same interface, you must configure a connectivity association with one secure channel for inbound traffic and a second secure channel for outbound traffic. The connectivity association is assigned to an interface later in this process.

For instance, to configure secure channel **sc1** to apply MACsec to incoming traffic:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 direction inbound
```

To configure secure channel **sc2** to apply MACsec to outgoing traffic:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc2 direction outbound
```

6. Specify a MAC address:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name id mac-address mac-address
```

If you are configuring a MAC address on a secure channel in the outbound direction, you should specify the MAC address of the interface as the **mac-address**.

If you are configuring a MAC address on a secure channel in the inbound direction, you should specify the MAC address of the interface at the other end of the link as the **mac-address**.

The **mac-address** variables must match on the sending and receiving secure channel on each side of a link to enable MACsec using static SAK security mode.



**NOTE:** You can see the MAC address of an interface in the **show interfaces** output.

To configure MACsec to accept frames from MAC address **12:34:56:ab:cd:ef** on secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 id mac-address
12:34:56:ab:cd:ef
```

7. Specify a port:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name id port-id port-id-number
```

The **port-id-number** variables must match on a sending and receiving secure channel on each side of a link to enable MACsec.



**NOTE:** The only requirement for port numbers in this implementation of MACsec is that they match on the sending and receiving ends of an Ethernet link. When the port numbers match, MACsec is enabled for all traffic on the connection.

To specify port ID 4 on secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 id port-id 4
```

8. (Optional) Enable encryption:

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name encryption
```

You can enable MACsec without enabling encryption. If a secure channel is configured on an interface without encryption, traffic is forwarded across the Ethernet link in clear text, and you will be able to view unencrypted data in the Ethernet frame traversing the link when you are monitoring it. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic on the link does not represent a security threat.

Encryption is disabled by default when you are enabling MACsec using static SAK security mode. To ensure all traffic traversing secure-channel **sc1** is encrypted:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 encryption
```

9. (Optional) Set an offset to send the first 30 or 50 octets in unencrypted plain text when encryption is enabled.

```
[edit security macsec]
user@switch# set connectivity-association connectivity-association-name secure-channel
secure-channel-name offset [0 | 30 | 50]
```

When the offset is set to 30, the IPv4 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic. When the offset is set to 50, the IPv6 header and the TCP/UDP header are unencrypted while encrypting the rest of the traffic.

You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.

The default offset is 0, so all traffic on the link is encrypted when the **encryption** option is enabled and an **offset** is not set.

To change the offset to 30 for secure channel **sc1**:

```
[edit security macsec]
user@switch# set connectivity-association ca1 secure-channel sc1 offset 30
```

10. Assign the connectivity association to an interface:

```
[edit security macsec]
user@switch# set interfaces interface-names connectivity-association
connectivity-association-name
```



Assigning the connectivity association to an interface is the final configuration step to enabling MACsec on an interface.

For instance, to assign connectivity association ca1 to interface xe-0/0/1:

```
[edit security macsec]
user@switch# set interfaces xe-0/1/0 connectivity-association ca1
```

MACsec using static SAK security mode is not enabled until a connectivity association on the opposite end of the link is also configured, and the configuration match on both ends of the link.

**Related  
Documentation**

- [Understanding Media Access Control Security \(MACsec\) on page 93](#)



## PART 4

# Using Port Security

- [Port Security on page 119](#)



## CHAPTER 4

# Port Security

- [Overview of Access Port Protection on page 119](#)
- [Understanding Port Security on page 122](#)
- [Understanding DHCP Snooping for Port Security on page 124](#)
- [Verifying That DHCP Snooping Is Working Correctly on page 131](#)
- [Understanding DAI for Port Security on page 132](#)
- [Verifying That DAI Is Working Correctly on page 135](#)
- [Understanding MAC Limiting and MAC Move Limiting for Port Security on page 135](#)
- [Verifying That MAC Limiting Is Working Correctly on page 137](#)
- [Verifying That MAC Move Limiting Is Working Correctly on page 140](#)
- [Verifying That the Port Error Disable Setting Is Working Correctly on page 141](#)
- [Understanding Trusted and Untrusted Ports on page 142](#)
- [Understanding Trusted DHCP Servers for Port Security on page 142](#)
- [Verifying That a Trusted DHCP Server Is Working Correctly on page 143](#)
- [Understanding DHCP Option 82 for Port Security on page 144](#)
- [Understanding Static ARP Entries on page 146](#)

## Overview of Access Port Protection

---

Port security features can protect a switch against various types of attacks. Protection methods against some common attacks are:

- [Mitigation of Ethernet Switching Table Overflow Attacks on page 119](#)
- [Mitigation of Rogue DHCP Server Attacks on page 120](#)
- [Protection Against ARP Spoofing Attacks on page 120](#)
- [Protection Against DHCP Snooping Database Alteration Attacks on page 121](#)
- [Protection Against DHCP Starvation Attacks on page 121](#)

## Mitigation of Ethernet Switching Table Overflow Attacks

In an overflow attack on an Ethernet switching table, an intruder sends so many requests from new MAC addresses that the table cannot learn all the addresses. The attack forces the switch to send broadcast messages when it needs to send traffic to addresses for

which it lacks MAC addresses. In addition to generating unnecessary traffic, the attacker might be able to sniff the broadcast packets.

To mitigate such attacks, you can configure a limit for learned MAC addresses or allow only specific MAC addresses. Use the MAC limit feature to control the total number of MAC addresses that can be added to the Ethernet switching table for the specified interface or interfaces. By setting the MAC addresses that are explicitly allowed, you ensure that the addresses of network devices whose network access is critical are guaranteed to be included in the Ethernet switching table.

## Mitigation of Rogue DHCP Server Attacks

By default, all access ports are untrusted, and all trunk ports are trusted with regard to DHCP. Trusted ports allow DHCP servers to provide IP addresses and other information to requesting devices. If someone connects an unauthorized DHCP server to a trusted port, the unauthorized server can start issuing IP addresses and configuration information to the network's DHCP clients. The information provided to the clients by this server can disrupt their network access. The unauthorized server might also assign itself as the default gateway device for the network. An attacker can then sniff the network traffic and perpetrate a man-in-the-middle attack—that is, it misdirects traffic intended for a legitimate network device to a device of its choice.

To mitigate this problem, set the interface to which the unauthorized server is connected as untrusted. That action blocks all ingress DHCP server messages from that interface.



**NOTE:** The switch logs all DHCP server packets that are received on untrusted ports. For example:

```
5 untrusted DHCP OFFER received, interface xe-0/0/2.0[65], vlan v1[10] server
ip/mac 12.12.12.1/00:00:00:00:01:12 offer ip/client mac
12.12.12.253/00:AA:BB:CC:DD:01
```

You can use these messages to detect unauthorized DHCP servers on the network.



**NOTE:** If you attach a DHCP server to an access port, you must configure the port as trusted.

---

## Protection Against ARP Spoofing Attacks

In ARP spoofing, an attacker sends faked ARP messages on the network. The attacker associates its own MAC address with the IP address of a network device connected to the switch. Any traffic sent to that IP address is instead sent to the attacker. Now the attacker can create various types of problems, including sniffing the packets that were meant for another host and perpetrating man-in-the-middle attacks. (In a man-in-the-middle attack, the attacker intercepts messages between two hosts, reads

them, and perhaps alters them, all without the original hosts knowing that their communications have been compromised.)

To protect against ARP spoofing on your switch, enable both DHCP snooping and dynamic ARP inspection (DAI). DHCP snooping builds and maintains the DHCP snooping table. That table contains the MAC addresses, IP addresses, lease times, binding types, VLAN information, and interface information for the untrusted interfaces on the switch. DAI uses the information in the DHCP snooping table to validate ARP packets. Invalid ARP packets are blocked, and when they are blocked, a system log message is recorded that includes the type of ARP packet and the sender's IP address and MAC address.

See *Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks*.

## Protection Against DHCP Snooping Database Alteration Attacks

In an attack designed to alter the DHCP snooping database, an intruder introduces a DHCP client on one of the switch's untrusted access interfaces that has a MAC address identical to that of a client on another untrusted port. The intruder acquires the DHCP lease, which results in changes to the entries in the DHCP snooping table. Subsequently, what would have been valid ARP requests from the legitimate client are blocked.

To protect against this type of alteration of the DHCP snooping database, configure MAC addresses that are explicitly allowed on the interface. See *Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks*.

## Protection Against DHCP Starvation Attacks

In a DHCP starvation attack, an attacker floods an Ethernet LAN with DHCP requests from spoofed (counterfeit) MAC addresses so that trusted DHCP servers cannot keep up with requests from legitimate DHCP clients. The address space of those servers is completely used up, so they can no longer assign IP addresses and lease times to clients. DHCP requests from those clients are either dropped—that is, the result is a denial of service (DoS)—or directed to a rogue DHCP server set up by the attacker to imitate a legitimate DHCP server.

To protect the switch from DHCP starvation attacks, use the MAC limiting feature. Specify the maximum number of MAC addresses that the switch can learn on the access interfaces to which DHCP clients connect. The DHCP server or servers can then supply only the specified number of IP addresses over each of those interfaces. If a DHCP starvation attack occurs after the maximum number of IP addresses has been assigned, the attack fails.

### Related Documentation

- [Understanding MAC Limiting and MAC Move Limiting for Port Security on page 135](#)
- [Configuring MAC Limiting](#)
- [Verifying That MAC Limiting Is Working Correctly on page 137](#)
- [Understanding DHCP Option 82 for Port Security on page 144](#)
- [Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks](#)
- [Understanding DAI for Port Security on page 132](#)

## Understanding Port Security

---

Ethernet LANs are vulnerable to attacks such as address spoofing (forging) and Layer 2 denial of service (DoS) on network devices. Port security features help protect the access ports on your device against the loss of information and productivity that such attacks can cause.

The Juniper Networks Junos operating system (Junos OS) provides features to help secure ports on a device. Ports can be categorized as either trusted or untrusted. You apply policies appropriate to each category to protect ports against various types of attacks.

Basic port security features are enabled in the device's default configuration. You can configure additional features with minimal configuration steps.

Depending on the particular feature, you can configure the feature either on VLANs or bridge domain interfaces.

Port security features supported on switching devices are:

- DHCP snooping—Filters and blocks ingress Dynamic Host Configuration Protocol (DHCP) server messages on untrusted ports; builds and maintains a database of DHCP lease information, which is called the DHCP snooping database.



**NOTE:** DHCP snooping is not enabled in the default configuration of the switching device. DHCP snooping is enabled on a VLAN or bridge domain. The details of enabling DHCP snooping depend on the particular device.

- DHCPv6 snooping—DHCP snooping for IPv6.
- DHCP option 82—Also known as the DHCP Relay Agent Information option. This DHCPv4 feature helps protect the switching device against attacks such as spoofing of IP addresses and MAC addresses and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.
- DHCPv6 option 37—Option 37 is the remote ID option for DHCPv6 and is used to insert information about the network location of the remote host into DHCPv6 packets. You enable option 37 on a VLAN.



**NOTE:** DHCPv6 snooping with option 37 is not supported on the MX Series.

- DHCPv6 option 18—Option 18 is the circuit ID option for DHCPv6 and is used to insert information about the client port into DHCPv6 packets. This option includes other details that can be optionally configured, such as the prefix and the interface description.
- DHCPv6 option 16—Option 16 is the vendor ID option for DHCPv6 and is used to insert information about the vendor of the client hardware into DHCPv6 packets.



- Dynamic ARP inspection (DAI)—Prevents Address Resolution Protocol (ARP) spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made on the basis of the results of those comparisons. You enable DAI on a VLAN.
- IPv6 neighbor discovery inspection—Prevents IPv6 address spoofing attacks. Neighbor discovery requests and replies are compared against entries in the DHCPv6 snooping database, and filtering decisions are made on the basis of the results of those comparisons. You enable neighbor discovery inspection on a VLAN.
- IP source guard—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. With IP source guard enabled, the source IP address in the packet sent from an untrusted access interface is validated against the DHCP snooping database. If the packet cannot be validated, it is discarded. You enable IP source guard on a VLAN or bridge domain.



**NOTE:** IP source guard is not supported on the QFX Series.

- IPv6 source guard—IP source guard for IPv6.



**NOTE:** IPv6 source guard is not supported on the QFX Series.

- MAC limiting—Protects against flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). You can enable MAC limiting on an interface.
- MAC move limiting—(Not supported on EX9200) Tracks MAC movement and detects MAC spoofing on access ports. You enable this feature on a VLAN or bridge domain.
- Persistent MAC learning—Also known as sticky MAC. Persistent MAC learning enables interfaces to retain dynamically learned MAC addresses across switch reboots. You enable this feature on an interface.
- Trusted DHCP server—Configuring the DHCP server on a trusted port protects against rogue DHCP servers sending leases. You enable this feature on an interface (port). By default, access ports are untrusted, and trunk ports are trusted. (Access ports are the switch ports that connect to Ethernet endpoints such as user PCs and laptops, servers, and printers. Trunk ports are the switch ports that connect an Ethernet switch to other switches or to routers.)

#### Related Documentation

- *Security Features for EX Series Switches Overview*
- [Understanding DHCP Snooping for Port Security on page 124](#)
- *Understanding DHCP Snooping for Port Security*
- *Understanding IPv6 Neighbor Discovery Inspection*
- [Understanding DAI for Port Security on page 132](#)
- *Understanding IP Source Guard for Port Security on EX Series Switches*

- *Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches*
- *Understanding DHCP Option 82 for Port Security on Switching Devices*

## Understanding DHCP Snooping for Port Security

---

DHCP snooping enables the switching device, which can be either a switch or a router, to monitor and control DHCP messages received from untrusted devices connected to it. When DHCP snooping is enabled, the system snoops the DHCP messages to view DHCP lease information and builds and maintains a database of valid bindings between IP addresses and MAC address (IP-MAC bindings) called the DHCP snooping database. Only clients with valid bindings are allowed access to the network.

- [DHCP Snooping Basics on page 124](#)
- [DHCP Snooping Process on page 125](#)
- [DHCPv6 Snooping on page 126](#)
- [Rapid Commit for DHCPv6 on page 126](#)
- [DHCP Server Access on page 127](#)
- [Static IP Address Additions to the DHCP Snooping Database on page 130](#)
- [Snooping DHCP Packets That Have Invalid IP Addresses on page 130](#)
- [Prioritizing Snooped Packets on page 131](#)

### DHCP Snooping Basics

The Dynamic Host Configuration Protocol (DHCP) allocates IP addresses dynamically, *leasing* addresses to devices so that the addresses can be reused when no longer needed. Hosts and end devices that require IP addresses obtained through DHCP must communicate with a DHCP server across the LAN.

DHCP snooping acts as a guardian of network security by keeping track of valid IP addresses assigned to downstream network devices by a trusted DHCP server (the server is connected to a trusted network port).

By default, all trunk ports on the switch are trusted and all access ports are untrusted for DHCP snooping.

When DHCP snooping is enabled, the lease information from the switching device is used to create the DHCP snooping table, also known as the binding table. The table shows current IP-MAC bindings, as well as lease time, type of binding, names of associated VLANs, and associated interfaces.



**NOTE:** DHCP snooping is disabled in the default configuration of the switching device. You must explicitly enable DHCP snooping by setting `examine-dhcp` at the `[edit ethernet-switching-options secure-access-port]` hierarchy level.

Entries in the DHCP snooping database are updated in these events:

- When a DHCP client releases an IP address (sends a DHCPRELEASE message). In this event, the associated mapping entry is deleted from the database.
- If you move a network device from one VLAN to another. In this event, typically the device needs to acquire a new IP address. Therefore, its entry in the database, including its VLAN ID, is updated.
- When the lease time (timeout value) assigned by the DHCP server expires. In this event, the associated entry is deleted from the database.



**TIP:** By default, the IP-MAC bindings are lost when the switching device is rebooted and DHCP clients (the network devices, or hosts) must reacquire bindings. However, you can configure the bindings to persist by setting the `dhcp-snooping-file` statement to store the database file either locally or remotely.

You can configure the switching device to snoop DHCP server responses from particular VLANs only. This prevents spoofing of DHCP server messages.

You configure DHCP snooping per VLAN, not per interface (port). DHCP snooping is disabled by default on switching devices.

## DHCP Snooping Process

The basic process of DHCP snooping consists of the following steps:



**NOTE:** When DHCP snooping is enabled for a VLAN, all DHCP packets sent from the network devices in that VLAN are subjected to DHCP snooping. The final IP-MAC binding occurs when the DHCP server sends DHCPACK to the DHCP client.

1. The network device sends a DHCPDISCOVER packet to request an IP address.
2. The switching device forwards the packet to the DHCP server.
3. The server sends a DHCPOFFER packet to offer an address. If the DHCPOFFER packet is from a trusted interface, the switching device forwards the packet to the DHCP client.
4. The network device sends a DHCPREQUEST packet to accept the IP address. The switching device adds an IP-MAC placeholder binding to the database. The entry is considered a placeholder until a DHCPACK packet is received from the server. Until then, the IP address could still be assigned to some other host.
5. The server sends a DHCPACK packet to assign the IP address or a DHCPNAK packet to deny the address request.
6. The switching device updates the DHCP snooping database according to the type of packet received:

- If the switching device receives a DHCPACK packet, it updates lease information for the IP-MAC bindings in its database.
- If the switching device receives a DHCPNACK packet, it deletes the placeholder.



**NOTE:** The DHCP snooping database is updated only after the DHCPREQUEST packet has been sent.

For general information about the messages that the DHCP client and DHCP server exchange during the assignment of an IP address for the client, see the *Junos OS Administration Library for Routing Devices*.

## DHCPv6 Snooping

DHCPv6 snooping is the equivalent of DHCP snooping for IPv6. The process for DHCPv6 snooping is similar to that for DHCP snooping, but uses different names for the messages exchanged between the client and server to assign IPv6 addresses. [Table 15 on page 126](#) shows DHCPv6 messages and their DHCP equivalents.

**Table 15: DHCPv6 Messages and Equivalent DHCPv4 Messages**

| Sent by | DHCPv6 Messages         | Equivalent DHCP Messages |
|---------|-------------------------|--------------------------|
| Client  | SOLICIT                 | DHCPDISCOVER             |
| Server  | ADVERTISE               | DHCPOFFER                |
| Client  | REQUEST, RENEW, REBIND  | DHCPREQUEST              |
| Server  | REPLY                   | DHCPACK/DHCPNAK          |
| Client  | RELEASE                 | DHCPRELEASE              |
| Client  | INFORMATION-REQUEST     | DHCPINFORM               |
| Client  | DECLINE                 | DHCPDECLINE              |
| Client  | CONFIRM                 | none                     |
| Server  | RECONFIGURE             | DHCPFORCERENEW           |
| Client  | RELAY-FORW, RELAY-REPLY | none                     |

## Rapid Commit for DHCPv6

DHCPv6 provides for a Rapid Commit option (DHCPv6 option 14), which, when supported by the server and set by the client, shortens the exchange from a four-way relay to a two-message handshake. For more information about enabling the Rapid Commit option, see *Enabling DHCPv6 Rapid Commit Support*.

In the rapid commit process:

1. The DHCPv6 client sends out a SOLICIT message that contains a request that rapid assignment of address, prefix, and other configuration parameters be preferred.
2. If the DHCPv6 server supports rapid assignment, it responds with a REPLY message, which contains the assigned IPv6 address and prefix and other configuration parameters.

## DHCP Server Access

You can configure a switching device's access to the DHCP server in three ways:

- [Switching Device, DHCP Clients, and DHCP Server Are All on the Same VLAN on page 127](#)
- [Switching Device Acts as DHCP Server on page 128](#)
- [Switching Device Acts as Relay Agent on page 129](#)

### Switching Device, DHCP Clients, and DHCP Server Are All on the Same VLAN

When the switching device, DHCP clients, and DHCP server are *all members of the same VLAN*, the DHCP server can be connected to the switching device in one of two ways:

- The server is directly connected to the same switching device as the one connected to the DHCP clients (the hosts, or network devices, that are requesting IP addresses from the server). The VLAN is enabled for DHCP snooping to protect the untrusted access ports. The trunk port is configured by default as a trusted port. See [Figure 4 on page 128](#).
- The server is connected to an intermediary switching device (Switching Device 2). The DHCP clients are connected to Switching Device 1, which is connected through a trunk port to Switching Device 2. Switching Device 2 is being used as a transit device. The VLAN is enabled for DHCP snooping to protect the untrusted access ports. The trunk port is configured by default as a trusted port. As shown in [Figure 5 on page 128](#), ge-0/0/11 is a trusted trunk port.

Figure 4: DHCP Server Connected Directly to a Switching Device

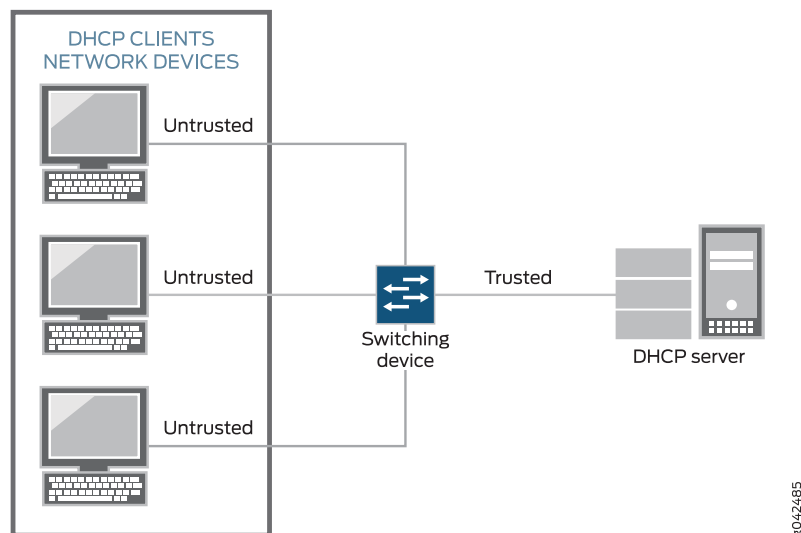
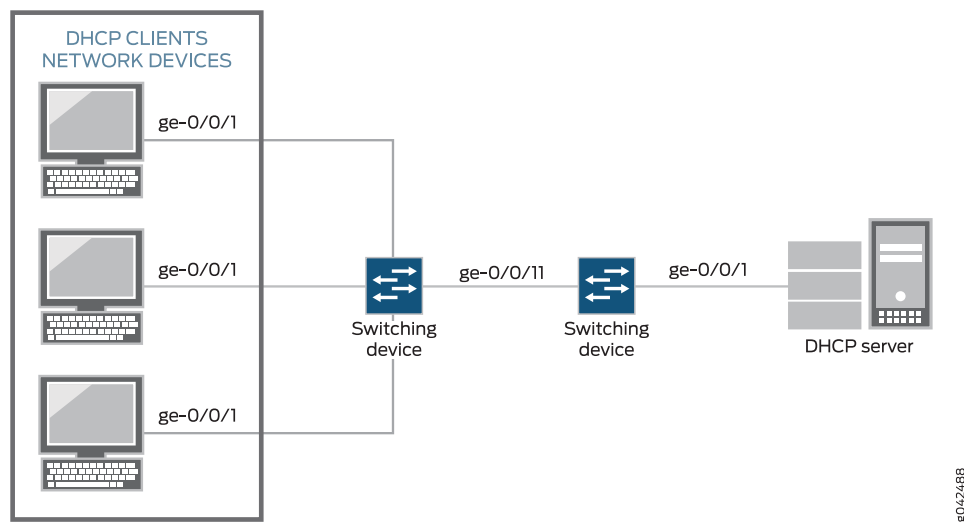


Figure 5: DHCP Server Connected Directly to Switching Device 2, with Switching Device 2 Connected to Switching Device 1 Through a Trusted Trunk Port



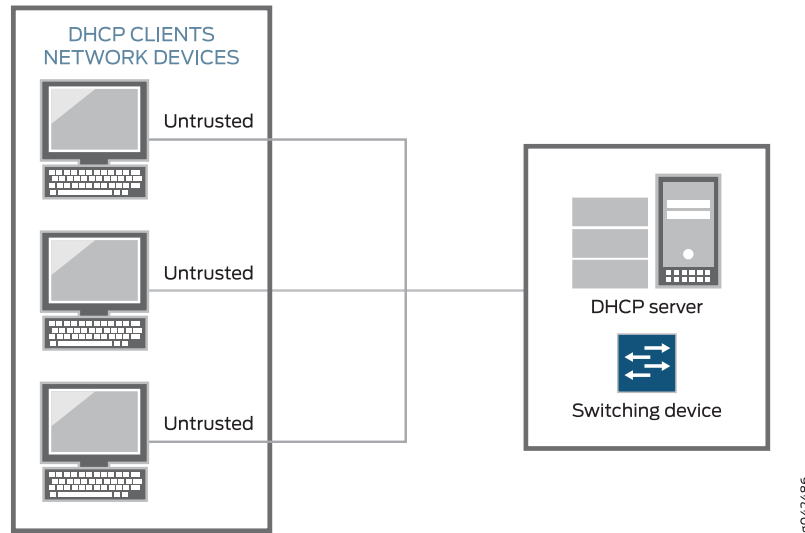
### Switching Device Acts as DHCP Server



**NOTE:** The switching device acting as a DHCP server is not supported on the QFX Series.

The switching device itself is configured as a DHCP server; this is known as a *local configuration*. See [Figure 6 on page 129](#).

**Figure 6: Switching Device Is the DHCP Server**



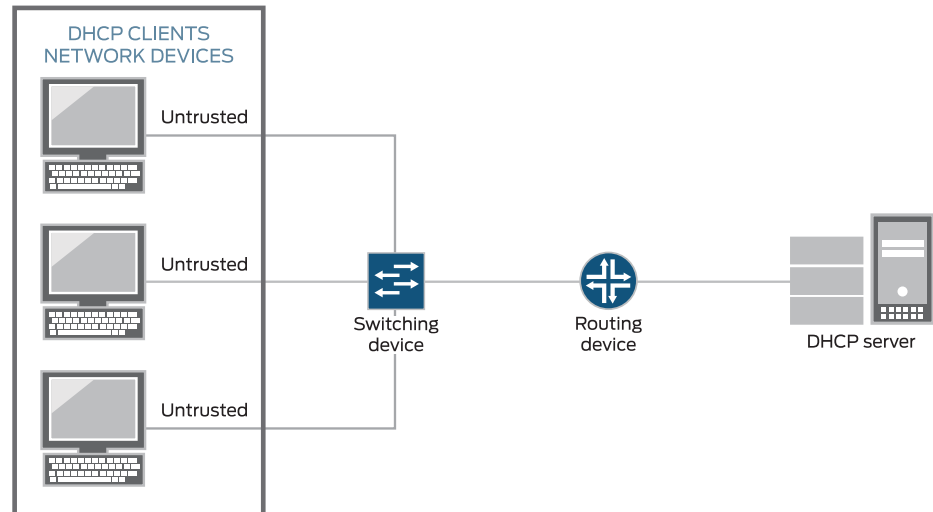
### Switching Device Acts as Relay Agent

The switching device functions as a relay agent when the DHCP clients or the DHCP server is connected to the device through a Layer 3 interface. The Layer 3 interfaces on the switching device are configured as routed VLAN interfaces (RVIs), which are also known as integrated routing and bridging (IRB) interfaces. The trunk interfaces are trusted by default.

These two scenarios illustrate the switching device acting as a relay agent:

- The DHCP server and clients are in different VLANs.
- The switching device is connected to a router that is in turn connected to the DHCP server. See [Figure 7 on page 130](#).

**Figure 7: Switching Device Acting as Relay Agent Through Router to DHCP Server**



8042487

## Static IP Address Additions to the DHCP Snooping Database

You can add specific static IP addresses to the database as well as have the addresses dynamically assigned through DHCP snooping. To add static IP addresses, you supply the IP address, the MAC address of the device, the interface on which the device is connected, and the VLAN with which the interface is associated. No lease time is assigned to the entry. The statically configured entry never expires.

## Snooping DHCP Packets That Have Invalid IP Addresses

If you enable DHCP snooping on a VLAN and then devices on that VLAN send DHCP packets that request invalid IP addresses, these invalid IP addresses are stored in the DHCP snooping database until they are deleted when their default timeout is reached. To eliminate this unnecessary consumption of space in the DHCP snooping database, the switching device drops the DHCP packets that request invalid IP addresses, preventing the snooping of these packets. The invalid IP addresses are:

- 0.0.0.0
- 128.0.x.x
- 191.255.x.x
- 192.0.0.x
- 223.255.255.x
- 224.x.x.x
- 240.x.x.x to 255.255.255.255



## Prioritizing Snooped Packets



**NOTE:** Prioritizing snooped packets is not supported on the QFX Series and the EX4600 switch.

You can use class-of-service (CoS) forwarding classes and queues to prioritize DHCP snooped packets for a specified VLAN. This type of configuration places the DHCP snooped packets for that VLAN in a specified egress queue, so that the security procedure does not interfere with the transmission of high-priority traffic. For additional information, see *Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic*.

- Related Documentation**
- [Understanding Port Security on page 122](#)
  - [Understanding Trusted DHCP Servers for Port Security on page 142](#)
  - [Enabling a Trusted DHCP Server on an MX Series Router \(CLI Procedure\)](#)
  - [Configuring Static IP Addresses for DHCP Bindings on Access Ports for MX Series Routers \(CLI Procedure\)](#)

## Verifying That DHCP Snooping Is Working Correctly

**Purpose** Verify that DHCP snooping is working on the switch and that the DHCP snooping database is correctly populated with both dynamic and static bindings.

**Action** Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the interface on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

```
user@switch> show dhcp snooping binding
```

DHCP Snooping Information:

| MAC address       | IP address | Lease (seconds) | Type    | VLAN     | Interface  |
|-------------------|------------|-----------------|---------|----------|------------|
| 00:05:85:3A:82:77 | 192.0.2.17 | 600             | dynamic | employee | ge-0/0/1.0 |
| 00:05:85:3A:82:79 | 192.0.2.18 | 653             | dynamic | employee | ge-0/0/1.0 |
| 00:05:85:3A:82:80 | 192.0.2.19 | 720             | dynamic | employee | ge-0/0/2.0 |
| 00:05:85:3A:82:81 | 192.0.2.20 | 932             | dynamic | employee | ge-0/0/2.0 |
| 00:05:85:3A:82:83 | 192.0.2.21 | 1230            | dynamic | employee | ge-0/0/2.0 |
| 00:05:85:27:32:88 | 192.0.2.22 | –               | static  | data     | ge-0/0/4.0 |

**Meaning** When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see preceding sample) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires. Static IP addresses have no assigned lease time. The statically configured entry never expires.

If the DHCP server had been configured as untrusted, no entries would be added to the DHCP snooping database and nothing would be shown in the output of the **show dhcp snooping binding** command.

**Related Documentation**

- [Enabling DHCP Snooping \(CLI Procedure\)](#)
- [Enabling DHCP Snooping \(J-Web Procedure\)](#)
- [Configuring Static IP Addresses in the DHCP Snooping Database for Access Ports \(CLI Procedure\)](#)
- [Example: Configuring Basic Port Security Features](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch](#)
- [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks](#)
- [Monitoring Port Security](#)
- [Troubleshooting Port Security](#)

---

## Understanding DAI for Port Security

Dynamic ARP inspection (DAI) protects switching devices against ARP spoofing.

DAI inspects Address Resolution Protocol (ARP) packets on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP spoofing (also known as ARP poisoning or ARP cache poisoning). ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons. When an attacker tries to use a forged ARP packet to spoof an address, the switch compares the address with entries in the database. If the media access control (MAC) address or IP address in the ARP packet does not match a valid entry in the DHCP snooping database, the packet is dropped.

ARP packets are sent to the Routing Engine and are rate-limited to protect the switching device from CPU overload.

- [Address Resolution Protocol on page 132](#)
- [ARP Spoofing on page 133](#)
- [Dynamic ARP Inspection on page 133](#)
- [Prioritizing Inspected Packets on page 134](#)

## Address Resolution Protocol

Sending IP packets on a multi-access network requires mapping an IP address to an Ethernet MAC address.

Ethernet LANs use ARP to map MAC addresses to IP addresses.

The switching device maintains this mapping in a cache that it consults when forwarding packets to network devices. If the ARP cache does not contain an entry for the destination device, the host (the DHCP client) broadcasts an ARP request for that device's address and stores the response in the cache.

## ARP Spoofing

ARP spoofing is one way to initiate man-in-the-middle attacks. The attacker sends an ARP packet that spoofs the MAC address of another device on the LAN. Instead of the switching device sending traffic to the proper network device, it sends the traffic to the device with the spoofed address that is impersonating the proper device. If the impersonating device is the attacker's machine, the attacker receives all the traffic from the switch that must have gone to another device. The result is that traffic from the switching device is misdirected and cannot reach its proper destination.

One type of ARP spoofing is gratuitous ARP, which is when a network device sends an ARP request to resolve its own IP address. In normal LAN operation, gratuitous ARP messages indicate that two devices have the same MAC address. They are also broadcast when a network interface card (NIC) in a device is changed and the device is rebooted, so that other devices on the LAN update their ARP caches. In malicious situations, an attacker can poison the ARP cache of a network device by sending an ARP response to the device that directs all packets destined for a certain IP address to go to a different MAC address instead.

To prevent MAC spoofing through gratuitous ARP and through other types of spoofing, the switches examine ARP responses through DAI.

## Dynamic ARP Inspection

DAI examines ARP requests and responses on the LAN and validates ARP packets. The switch intercepts ARP packets from an access port and validates them against the DHCP snooping database. If no IP-MAC entry in the database corresponds to the information in the ARP packet, DAI drops the ARP packet and the local ARP cache is not updated with the information in that packet. DAI also drops ARP packets when the IP address in the packet is invalid. ARP probe packets are not subjected to dynamic ARP inspection. The switch always forwards such packets.

Junos OS for EX Series switches and the QFX Series uses DAI for ARP packets received on access ports because these ports are untrusted by default. Trunk ports are trusted by default, and therefore ARP packets bypass DAI on them.

You configure DAI for each VLAN, not for each interface (port). By default, DAI is disabled for all VLANs.

If you set an interface to be a DHCP trusted port, it is also trusted for ARP packets.

**NOTE:**

- If your switching device is an EX Series switch and uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style, see *Enabling a Trusted DHCP Server (CLI Procedure)* for information about configuring an access interface to be a DHCP trusted port.
- If your switching device is an EX Series switch and is *not* using Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style, see *Enabling a Trusted DHCP Server (CLI Procedure)* for information about configuring an access interface to be a DHCP trusted port.

For packets directed to the switching device to which a network device is connected, ARP queries are broadcast on the VLAN. The ARP responses to those queries are subjected to the DAI check.

For DAI, all ARP packets are trapped to the Packet Forwarding Engine. To prevent CPU overloading, ARP packets destined for the Routing Engine are rate-limited.

If the DHCP server goes down and the lease time for an IP-MAC entry for a previously valid ARP packet runs out, that packet is blocked.

## Prioritizing Inspected Packets



**NOTE:** Prioritizing inspected packets is not supported on the QFX Series and the EX4600 switch.

You can use class-of-service (CoS) forwarding classes and queues to prioritize DAI packets for a specified VLAN. This type of configuration places inspected packets for that VLAN in the egress queue, that you specify, ensuring that the security procedure does not interfere with the transmission of high-priority traffic.

**Related Documentation**

- [Understanding Port Security on page 122](#)
- [Understanding DHCP Snooping for Port Security on page 124](#)
- [Example: Configuring Basic Port Security Features](#)
- [Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch](#)
- [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks](#)
- [Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing](#)
- [Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic](#)
- [Enabling Dynamic ARP Inspection \(CLI Procedure\)](#)

- [Enabling Dynamic ARP Inspection \(CLI Procedure\)](#)
- [Enabling Dynamic ARP Inspection \(J-Web Procedure\)](#)

## Verifying That DAI Is Working Correctly

**Purpose** Verify that dynamic ARP inspection (DAI) is working on the switch.

**Action** Send some ARP requests from network devices connected to the switch.

Display the DAI information:

```
user@switch> show arp inspection statistics
ARP inspection statistics:
Interface Packets received ARP inspection pass ARP inspection failed

ge-0/0/1.0 7 5 2
ge-0/0/2.0 10 10 0
ge-0/0/3.0 12 12 0
```

**Meaning** The sample output shows the number of ARP packets received and inspected per interface, with a listing of how many packets passed and how many failed the inspection on each interface. The switch compares the ARP requests and replies against the entries in the DHCP snooping database. If a MAC address or IP address in the ARP packet does not match a valid entry in the database, the packet is dropped.

- Related Documentation**
- [Enabling Dynamic ARP Inspection \(CLI Procedure\)](#)
  - [Enabling Dynamic ARP Inspection \(J-Web Procedure\)](#)
  - [Example: Configuring Basic Port Security Features](#)
  - [Example: Configuring DHCP Snooping, DAI , and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch](#)
  - [Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks](#)
  - [Monitoring Port Security](#)

## Understanding MAC Limiting and MAC Move Limiting for Port Security

MAC limiting protects against flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). You enable this feature on Layer 2 interfaces (ports). MAC move limiting detects MAC movement and MAC spoofing on access interfaces. You enable this feature on VLANs.

- [MAC Limiting on page 136](#)
- [MAC Move Limiting on page 136](#)
- [Actions for MAC Limiting on page 137](#)
- [MAC Addresses That Exceed the MAC Limit or MAC Move Limit on page 137](#)

## MAC Limiting

MAC limiting sets a limit on the number of MAC addresses that can be learned on a single Layer 2 access interface or on all the Layer 2 access interfaces on the switch. Junos OS provides two MAC limiting methods:

- Maximum number of MAC addresses—You configure the maximum number of dynamic MAC addresses allowed per interface. When the limit is exceeded, incoming packets with new MAC addresses can be ignored, dropped, or logged. You can also specify that the interface be shut down or temporarily disabled.
- Allowed MAC addresses—You configure specific “allowed” MAC addresses for the access interface. Any MAC address that is not in the list of configured addresses is not learned, and the switch logs an appropriate message. Allowed MAC binds MAC addresses to a VLAN so that the address does not get registered outside the VLAN. If an allowed MAC setting conflicts with a dynamic MAC setting, the allowed MAC setting takes precedence.



**NOTE:** If you do not want the system to log messages about invalid MAC addresses received by an interface that has been configured for allowed MAC addresses, disable the logging by configuring the `no-allowed-mac-log` statement.

You configure MAC limiting per interface, not per VLAN. You can specify the maximum number of dynamic MAC addresses that can be learned on a single Layer 2 access interface (including tagged-access interfaces) or on all Layer 2 access interfaces.

## MAC Move Limiting

MAC move limiting causes the switch to track the number of times a MAC address can move to a new interface (port). It can help to prevent MAC spoofing, and it can also detect and prevent loops.

If a MAC address moves more than the configured number of times within 1 second, the switch performs the configured action. You can configure MAC move limiting to apply to all VLANs or to a specific VLAN.



**CAUTION:** Mac move limiting does not work properly on a QFX5100 switch used as a Node device in a QFabric system. Do not use this feature on a QFX5100 switch in a QFabric system.

## Actions for MAC Limiting

You can choose to have one of the following actions performed when the limit of MAC addresses or the limit of MAC moves is exceeded:

- **drop**—Drop the packet and generate a system log entry. This is the default.
- **log**—Do not drop the packet but generate a system log entry.
- **none**—Take no action.
- **shutdown**—Disable the interface and generate an alarm. If you configure the switch with the **port-error-disable** statement, the disabled interface recovers automatically upon expiration of the specified timeout. If this is not configured, you can bring up the disabled interfaces by running the **clear ethernet-switching port-error** command.

See descriptions of results of these various action settings in [“Verifying That MAC Limiting Is Working Correctly” on page 137](#).

If you set a MAC limit to apply to all interfaces on the switch, you can override that setting for a particular interface by specifying action **none**. See *Configuring the none Action to Override a MAC Limit Applied to All Interfaces (CLI Procedure)*

## MAC Addresses That Exceed the MAC Limit or MAC Move Limit

If you have configured the **port-error-disable** statement, you can view which interfaces are temporarily disabled because the MAC limit or MAC move limit was exceeded. Use the **show ethernet-switching interfaces** command.

The log messages that indicate the MAC limit or MAC move limit has been exceeded include the offending MAC addresses.

### Related Documentation

- [Understanding Port Security on page 122](#)
- [Configuring MAC Limiting](#)
- [Configuring MAC Move Limiting \(CLI Procedure\)](#)
- [Verifying That MAC Limiting Is Working Correctly on page 137](#)
- [Verifying That MAC Move Limiting Is Working Correctly on page 140](#)
- [Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks](#)
- [Example: Configuring Basic Port Security Features](#)
- [no-allowed-mac-log on page 250](#)

## Verifying That MAC Limiting Is Working Correctly

MAC limiting protects against flooding of the Ethernet switching table by setting a limit on the number of MAC addresses that can be learned on a single Layer 2 access interface (port).

Junos OS provides two MAC limiting methods:

- **Maximum number of MAC addresses**—You configure the maximum number of dynamic MAC addresses allowed per interface. When the limit is exceeded, incoming packets with new MAC addresses can be ignored, dropped, or logged. You can also specify that the interface be shut down or temporarily disabled.
- **Allowed MAC addresses**—You configure specific “allowed” MAC addresses for the access interface. Any MAC address that is not in the list of configured addresses is not learned, and the switch logs an appropriate message. The allowed MAC method binds MAC addresses to a VLAN so that the address is not registered outside the VLAN. If an allowed MAC setting conflicts with a dynamic MAC setting, the allowed MAC setting takes precedence.

This topic includes the following tasks:

1. [Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly on page 138](#)
2. [Verifying That Allowed MAC Addresses Are Working Correctly on page 138](#)
3. [Verifying That Interfaces Are Shut Down on page 139](#)
4. [Customizing the Ethernet Switching Table Display to View Information for a Specific Interface on page 140](#)

## Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly

**Purpose** Verify that MAC limiting for dynamic MAC addresses is working.

**Action** Display the MAC addresses that have been learned. The following sample output shows the results of sending two packets from hosts connected to **xe-1:0/0/1** and five packets from hosts connected to **xe-1:0/0/2**, with both interfaces configured with a MAC limit of **4** and the action **drop**:

```
user@switch> show ethernet-switching table
Ethernet-switching table: 7 entries, 6 learned
```

| VLAN          | MAC address       | Type  | Age | Interfaces   |
|---------------|-------------------|-------|-----|--------------|
| employee-vlan | *                 | Flood | –   | xe-1:0/0/2.0 |
| employee-vlan | 00:05:85:3A:82:77 | Learn | 0   | xe-1:0/0/1.0 |
| employee-vlan | 00:05:85:3A:82:79 | Learn | 0   | xe-1:0/0/1.0 |
| employee-vlan | 00:05:85:3A:82:80 | Learn | 0   | xe-1:0/0/2.0 |
| employee-vlan | 00:05:85:3A:82:81 | Learn | 0   | xe-1:0/0/2.0 |
| employee-vlan | 00:05:85:3A:82:83 | Learn | 0   | xe-1:0/0/2.0 |
| employee-vlan | 00:05:85:3A:82:85 | Learn | 0   | xe-1:0/0/2.0 |

**Meaning** The output shows that the fifth packet received on the **xe-1:0/0/2** interface was dropped because it exceeded the MAC limit for that interface. The address was not learned, and thus an asterisk (\*) rather than an address appears in the MAC address column in the first line of the sample output.

## Verifying That Allowed MAC Addresses Are Working Correctly

**Purpose** Verify that allowed MAC addresses are working.



**Action** Display the MAC cache information after allowed MAC addresses have been configured on an interface. The following sample shows the MAC cache after four allowed MAC addresses had been configured on interface **xe-1:0/0/2** and a fifth MAC address appeared on the interface.

```
user@switch> show ethernet-switching table
Ethernet-switching table: 5 entries, 4 learned
```

| VLAN          | MAC address       | Type  | Age | Interfaces   |
|---------------|-------------------|-------|-----|--------------|
| employee-vlan | 00:05:85:3A:82:80 | Learn | 0   | xe-1:0/0/2.0 |
| employee-vlan | 00:05:85:3A:82:81 | Learn | 0   | xe-1:0/0/2.0 |
| employee-vlan | 00:05:85:3A:82:83 | Learn | 0   | xe-1:0/0/2.0 |
| employee-vlan | 00:05:85:3A:82:85 | Learn | 0   | xe-1:0/0/2.0 |
| employee-vlan | *                 | Flood | -   | xe-1:0/0/2.0 |

**Meaning** Because the fifth address was not allowed it was not learned, and an asterisk (\*) rather than an address appears in the MAC address column in the last line of the sample output.

## Verifying That Interfaces Are Shut Down

**Purpose** Verify that an interface is shut down when the MAC limit is exceeded.

**Action** For more information about interfaces that have been shut down because the MAC limit was exceeded, use the **show ethernet-switching interfaces** command.

```
user@switch> show ethernet-switching interfaces
```

| Interface   | State | VLAN members | Tag      | Tagging            | Blocking |
|-------------|-------|--------------|----------|--------------------|----------|
| bme0.32770  | down  | mgmt         | untagged | unblocked          |          |
| xe-0/0/0.0  | down  | v1           | untagged | MAC limit exceeded |          |
| xe- 0/0/1.0 | up    | v1           | untagged | unblocked          |          |
| xe-0/0/2.0  | up    | v1           | untagged | unblocked          |          |
| me0.0       | up    | mgmt         | untagged | unblocked          |          |



**NOTE:** You can configure interfaces to recover automatically when the MAC limit has been exceeded by specifying the **port-error-disable** statement with a **disable timeout** value. The switch automatically restores the disabled interface to service when the disable timeout expires. The **port-error-disable** configuration does not apply to preexisting error conditions—it affects only error conditions that are detected after the **port-error-disable** statement has been enabled and the configuration has been committed. To clear a preexisting error condition and restore the interface to service, use the **clear ethernet-switching port-error** command.

## Customizing the Ethernet Switching Table Display to View Information for a Specific Interface

**Purpose** You can use the **show ethernet-switching table** command to view information for a specific interface.

**Action** For example, to display the MAC addresses that have been learned on the **xe-0/0/2** interface, enter:

```
user@switch> show ethernet-switching table interface xe-0/0/2.0
Ethernet-switching table: 1 unicast entries
```

| VLAN | MAC address       | Type  | Age | Interfaces  |
|------|-------------------|-------|-----|-------------|
| v1   | *                 | Flood | -   | All-members |
| v1   | 00:00:06:00:00:00 | Learn | 0   | xe-0/0/2.0  |

**Meaning** The MAC limit value for the **xe-0/0/2** interface had been set to 1, and the output shows that only one MAC address was learned and added to the MAC cache.

- Related Documentation**
- *Configuring MAC Limiting*
  - *Monitoring Port Security*
  - *Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)*
  - *Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks*
  - *Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks*

---

## Verifying That MAC Move Limiting Is Working Correctly

**Purpose** Verify that MAC move limiting is working on the switch.

**Action** Display the MAC addresses in the Ethernet switching table when MAC move limiting has been configured for a VLAN. The following sample shows the results after two of the hosts on **ge-0/0/2** sent packets after the MAC addresses for those hosts had moved to other interfaces more than five times in 1 second. The VLAN, **employee-vlan**, was set to a MAC move limit of 5 with the action **drop**:

```
user@switch> show ethernet-switching table
```

```
Ethernet-switching table: 7 entries, 4 learned
```

| VLAN          | MAC address       | Type  | Age | Interfaces |
|---------------|-------------------|-------|-----|------------|
| employee-vlan | 00:05:85:3A:82:77 | Learn | 0   | ge-0/0/1.0 |
| employee-vlan | 00:05:85:3A:82:79 | Learn | 0   | ge-0/0/1.0 |
| employee-vlan | 00:05:85:3A:82:80 | Learn | 0   | ge-0/0/2.0 |
| employee-vlan | 00:05:85:3A:82:81 | Learn | 0   | ge-0/0/2.0 |
| employee-vlan | *                 | Flood | -   | ge-0/0/2.0 |
| employee-vlan | *                 | Flood | -   | ge-0/0/2.0 |

**Meaning** The last two lines of the sample output show that MAC addresses for two hosts on **ge-0/0/2** were not learned, because the hosts had been moved back and forth from the original interfaces more than five times in 1 second.

- Related Documentation**
- *Configuring MAC Move Limiting (CLI Procedure)*
  - *Configuring MAC Move Limiting (J-Web Procedure)*
  - *Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)*
  - *Example: Configuring Basic Port Security Features*
  - *Monitoring Port Security*

## Verifying That the Port Error Disable Setting Is Working Correctly

**Purpose** Verify that the port error disable setting is working as expected for MAC limited and storm control interfaces.

**Action** Display information about interfaces:

```
user@switch> show ethernet-switching interfaces
```

| Interface    | State | VLAN members | Blocking                |
|--------------|-------|--------------|-------------------------|
| xe-2:0/0/0.0 | up    | T1122        | unblocked               |
| xe-2:0/0/1.0 | down  | default      | MAC limit exceeded      |
| xe-2:0/0/2.0 | down  | default      | Storm control in effect |
| xe-2:0/0/3.0 | down  | default      | unblocked               |
| xe-2:0/0/4.0 | down  | default      | unblocked               |
| xe-2:0/0/5.0 | down  | default      | unblocked               |
| xe-2:0/0/6.0 | down  | default      | unblocked               |

**Meaning** For interfaces disabled by port security features, the sample output from the **show ethernet-switching interfaces** command specifies the reasons that the interfaces are disabled:

- **MAC limit exceeded**—The interface is temporarily disabled because of a *mac-limit* error. The disabled interface is automatically restored to service when the *disable-timeout* (*Port Error Disable*) expires.
- **MAC move limit exceeded**—The interface is temporarily disabled because of a *mac-move-limit* error. The disabled interface is automatically restored to service when the *disable-timeout* expires.
- **Storm control in effect**—The interface is temporarily disabled because of a *storm-control* error. The disabled interface is automatically restored to service when the *disable-timeout* (*Port Error Disable*) expires.

**Related  
Documentation**

- [Understanding MAC Limiting and MAC Move Limiting for Port Security on page 135](#)
- [port-error-disable on page 252](#)
- [Configuring Autorecovery for MAC Limited or Storm Control Interfaces \(CLI Procedure\)](#)

---

## Understanding Trusted and Untrusted Ports

---

By default, all access ports are untrusted and all trunk ports are trusted in regard to DHCP. Trusted ports allow DHCP servers to provide IP addresses and other information to requesting devices. Untrusted ports drop traffic from DHCP servers to prevent unauthorized servers from providing any configuration information to clients.

If you attach a DHCP server to an access port, you must configure the port as trusted. Before you do so, ensure that the server is physically secure—that is, that access to the server is monitored and controlled.

**Related  
Documentation**

- [Understanding DHCP Snooping for Port Security on page 124](#)
- [Example: Configuring Basic Port Security Features](#)
- [Enabling a Trusted Port for DHCP](#)

---

## Understanding Trusted DHCP Servers for Port Security

---

Any interface on the switching device that connects to a DHCP server can be configured as a trusted port. Configuring a DHCP server on a trusted port protects against rogue DHCP servers sending leases.

Ensure that the DHCP server interface is physically secure—that is, that access to the server is monitored and controlled at the site—before you configure the port as trusted.

**Related  
Documentation**

- [Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks](#)
- [Enabling a Trusted DHCP Server \(CLI Procedure\)](#)

## Verifying That a Trusted DHCP Server Is Working Correctly

**Purpose** Verify that a DHCP trusted server is working on the switch. See what happens when the DHCP server is trusted and then untrusted.

**Action** Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the interface on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

```
user@switch> show dhcp snooping binding
```

DHCP Snooping Information:

| MAC Address       | IP Address | Lease | Type    | VLAN          | Interface  |
|-------------------|------------|-------|---------|---------------|------------|
| 00:05:85:3A:82:77 | 192.0.2.17 | 600   | dynamic | employee-vlan | ge-0/0/1.0 |
| 00:05:85:3A:82:79 | 192.0.2.18 | 653   | dynamic | employee-vlan | ge-0/0/1.0 |
| 00:05:85:3A:82:80 | 192.0.2.19 | 720   | dynamic | employee-vlan | ge-0/0/2.0 |
| 00:05:85:3A:82:81 | 192.0.2.20 | 932   | dynamic | employee-vlan | ge-0/0/2.0 |
| 00:05:85:3A:82:83 | 192.0.2.21 | 1230  | dynamic | employee-vlan | ge-0/0/2.0 |
| 00:05:85:27:32:88 | 192.0.2.22 | 3200  | dynamic | employee-vlan | ge-0/0/2.0 |

**Meaning** When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see preceding sample) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires.

If the DHCP server had been configured as untrusted, no entries would be added to the DHCP snooping database and nothing would be shown in the output of the **show dhcp snooping binding** command.

- Related Documentation**
- *Enabling a Trusted DHCP Server (CLI Procedure)*
  - *Enabling a Trusted Port for DHCP*
  - *Example: Configuring Basic Port Security Features*
  - *Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks*
  - *Monitoring Port Security*
  - *Troubleshooting Port Security*

## Understanding DHCP Option 82 for Port Security

---

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect the switch against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation. Hosts on untrusted access interfaces on Ethernet LAN switches send requests for IP addresses in order to access the Internet. The switch forwards or relays these requests to DHCP servers, and the servers send offers for IP address leases in response. Attackers can use these messages to perpetrate address spoofing and starvation.

Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client. The Juniper Networks Junos operating system (Junos OS) implementation of DHCP option 82 supports RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>.

This topic covers:

- [DHCP Option 82 Processing on page 144](#)
- [Suboption Components of Option 82 on page 145](#)
- [Configurations That Support Option 82 on page 145](#)

### DHCP Option 82 Processing

If DHCP option 82 is enabled on the switch, then when a DHCP client that is connected to the switch on an untrusted interface sends a DHCP request, the switch inserts information about the client's network location into the packet header of that request. The switch then sends the request to the DHCP server. The DHCP server reads the option 82 information in the packet header and uses it to implement the IP address or another parameter for the client. See “[Suboption Components of Option 82](#)” on [page 145](#) for details about option 82 information.

You can enable DHCP option 82 on a single VLAN or on all VLANs on the switch. You can also configure it on Layer 3 interfaces (in routed VLAN interfaces, or RVIs) when the switch is functioning as a relay agent.

When option 82 is enabled on the switch, then this sequence of events occurs when a DHCP client sends a DHCP request:

1. The switch receives the request and inserts the option 82 information in the packet header.
2. The switch forwards or relays the request to the DHCP server.
3. The server uses the DHCP option 82 information to formulate its reply and sends a response back to the switch. It does not alter the option 82 information.
4. The switch strips the option 82 information from the response packet.
5. The switch forwards the response packet to the client.



**NOTE:** To use the DHCP option 82 feature, you must ensure that the DHCP server is configured to accept option 82. If it is not configured to accept option 82, then when it receives requests containing option 82 information, it does not use the information in setting parameters and it does not echo the information in its response message.

## Suboption Components of Option 82

When configuring DHCP option 82, you can use the following suboptions:

- **circuit ID**—Identifies the circuit (interface and/or VLAN) on the switch on which the request was received. The circuit ID contains the interface name and/or VLAN name, with the two elements separated by a colon—for example, **xe-0/0/10:vlan1**. If the request packet is received on a Layer 3 interface, the circuit ID is just the interface name—for example, **xe-0/0/10**.

Use the **prefix** option to add an optional prefix to the circuit ID. If you enable the **prefix** option, the hostname for the switch is used as the prefix; for example, **switch1:xe-0/0/10:vlan1**.

You can also specify that the interface description be used rather than the interface name and that the VLAN ID be used rather than the VLAN name.

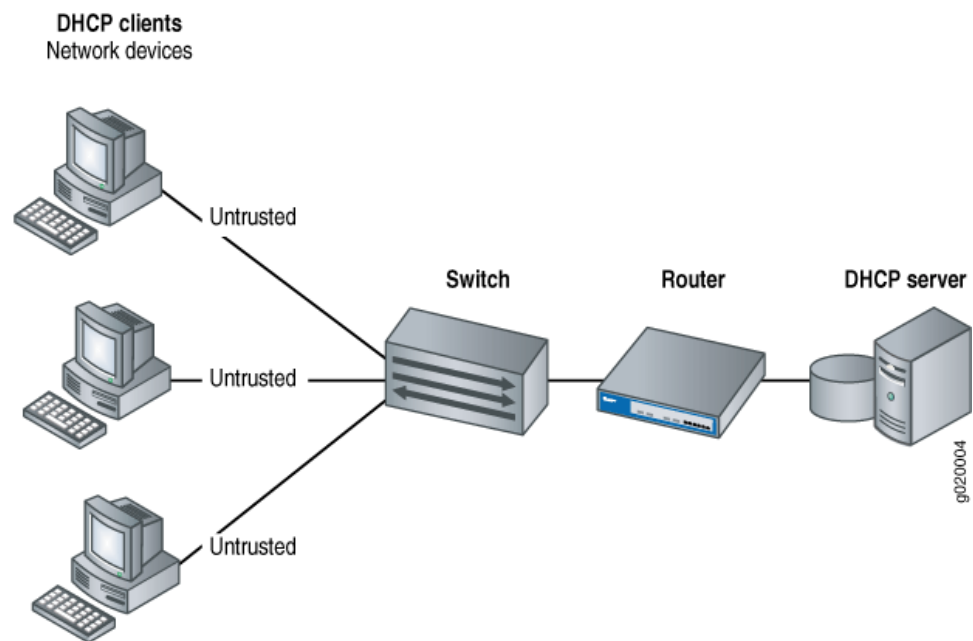
- **remote ID**—Identifies the host. By default, the remote ID is the MAC address of the switch. You can specify that the remote ID be the hostname of the switch, the interface description, or a character string of your choice. You can also add an optional prefix to the remote ID.
- **vendor ID**—Identifies the vendor of the host. If you specify the **vendor-id** option but do not enter a value, the default value **Juniper** is used. To specify a value, you type a character string.

## Configurations That Support Option 82

You can use option 82 with the following configurations:

- The DHCP client and the DHCP server are on the same VLAN. In this case the switch forwards the requests from the clients on untrusted access interfaces to the server on a trusted interface. For this configuration, you set DHCP option 82 at the **[edit ethernet-switching-options secure-access-port vlan]** hierarchy level.
- The DHCP client or the DHCP server is connected to the switch through a Layer 3 interface and the switch is configured to relay DHCP requests. [Figure 8 on page 146](#) illustrates a scenario for the switch-as-relay-agent; in this instance, the switch relays requests through a router to the server.

Figure 8: Switch Relays DHCP Requests to Server



For the configuration shown in [Figure 8 on page 146](#), you set DHCP option 82 at the **[edit forwarding-options helpers bootp]** hierarchy level.

#### Related Documentation

- [Overview of Access Port Protection on page 119](#)
- [DHCP and BOOTP Relay Overview](#)
- [dhcp-option82](#)
- [Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server](#)
- [Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server](#)
- [Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server \(CLI Procedure\)](#)
- [Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server \(CLI Procedure\)](#)

## Understanding Static ARP Entries

You can create explicit mappings between IP addresses and MAC addresses, which are called static ARP table entries. Unlike dynamically learned ARP entries, static entries do not age out. You might want to create static ARP entries in a troubleshooting situation or if your device is unable to learn a MAC address dynamically for any reason.

#### Related Documentation

- [Configuring Static ARP Entries](#)



- *arp*



## PART 5

# Using Device Security

- [Device Security on page 151](#)



## CHAPTER 5

# Device Security

- [Understanding Storm Control on page 151](#)
- [Understanding Unicast RPF on page 153](#)
- [Understanding Unknown Unicast Forwarding on page 157](#)
- [Example: Configuring Storm Control to Prevent Network Outages on page 157](#)
- [Verifying That the Port Error Disable Setting Is Working Correctly on page 159](#)
- [Configuring Unicast RPF \(CLI Procedure\) on page 160](#)
- [Disabling Unicast RPF \(CLI Procedure\) on page 162](#)
- [Verifying Unicast RPF Status on page 162](#)
- [Configuring Unknown Unicast Forwarding \(CLI Procedure\) on page 165](#)

### Understanding Storm Control

---

A traffic storm occurs when broadcast packets prompt receiving devices to broadcast packets in response. This prompts further responses, creating a snowball effect. The switch is flooded with packets, which creates unnecessary traffic that leads to poor performance or even a complete loss of service by some clients. Storm control causes a device to monitor traffic levels and take a specified action when a specified traffic level—called the *storm control level*—is exceeded, thus preventing packets from proliferating and degrading service. You can configure devices to drop broadcast and unknown unicast packets, shut down interfaces, or temporarily disable interfaces when the storm control level is exceeded.

Storm control is enabled by default on ELS platforms and disabled by default on non-ELS platforms. If storm control is enabled, the default level is 80 percent of the available bandwidth for ingress traffic. You can change the storm control level by configuring it as a specific bandwidth value. (The **level** configuration statement, which allows you to configure the storm control level as a percentage of the combined broadcast and unknown unicast streams, is deprecated and might be removed from future releases. We recommend that you phase out its use and replace it with the **bandwidth** statement.)



---

**NOTE:** Storm control is not enabled by default on MX platforms.

---



**NOTE:** When you configure storm control bandwidth, the value you configure is rounded off internally to the closest multiple of 64 Kbps, and the rounded-off value represents the bandwidth that is actually enforced. For example, if you configure a bandwidth limit of 150 Kbps, storm control enforces a bandwidth limit of 128 Kbps.



**NOTE:** On an FCoE-FC gateway, storm control must be disabled on all Ethernet interfaces that belong to an FCoE VLAN to prevent FCoE traffic from being dropped. Configuring storm control on an Ethernet interface that is included in an FCoE-FC gateway may have undesirable effects, including FCoE packet loss. After disabling storm control on all interfaces, enable storm control on any interfaces that are not part of an FCoE-FC gateway on which you want to use storm control. However, on an FCoE transit switch, you can enable storm control on interfaces that carry FCoE traffic.



**CAUTION:** The Junos OS allows you to configure a storm control value that exceeds the bandwidth of the interface. If you configure an interface this way, storm control does not drop broadcast or unknown unicast packets even if they consume all the available bandwidth.

To recognize a storm, you must be able to identify when traffic has reached an abnormal level. Suspect a storm when operations begin timing out and network response times slow down. Users might be unable to access expected services. Monitor the percentage of broadcast and unknown unicast traffic in the network when it is operating normally. This data can then be used as a benchmark to determine when traffic levels are too high. You can then configure storm control to set the level at which you want to drop broadcast and unknown unicast traffic.

#### Related Documentation

- *Example: Configuring Storm Control to Prevent Network Outages*
- *Example: Configuring Storm Control on an OVSDB-Managed Interface*
- *Configuring Autorecovery for MAC Limited or Storm Control Interfaces (CLI Procedure)*
- *Disabling Storm Control on FCoE Interfaces on an FCoE-FC Gateway*
- [action-shutdown on page 258](#)
- *interface (Storm Control)*
- [port-error-disable on page 252](#)
- *storm-control*

## Understanding Unicast RPF

Unicast reverse-path forwarding (RPF) helps protect the switch against denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks by verifying the unicast source address of each packet that arrives on an ingress interface where unicast RPF is enabled. It also helps ensure that traffic arriving on ingress interfaces comes from a network source that the receiving interface can reach.

When you enable unicast RPF, the switch forwards a packet only if the receiving interface is the best return path to the packet's unicast source address. This is known as strict mode unicast RPF.



**NOTE:** On Juniper Networks EX3200, EX4200, EX4300, and EX4500 Ethernet Switches, the switch applies unicast RPF *globally* to all interfaces when unicast RPF is configured on any interface. For additional information, see [“Limitations of the Unicast RPF Implementation on EX3200, EX4200, EX4300, and EX4500 Switches” on page 156.](#)

This topic covers:

- [Unicast RPF for Switches Overview on page 153](#)
- [Unicast RPF Implementation on page 154](#)
- [When to Enable Unicast RPF on page 154](#)
- [When Not to Enable Unicast RPF on page 155](#)
- [Limitations of the Unicast RPF Implementation on EX3200, EX4200, EX4300, and EX4500 Switches on page 156](#)

### Unicast RPF for Switches Overview

Unicast RPF functions as an ingress filter that reduces the forwarding of IP packets that might be spoofing an address. By default, unicast RPF is disabled on the switch interfaces.

The type of unicast RPF provided on the switches—that is, strict mode unicast RPF is especially useful on untrusted interfaces. An untrusted interface is an interface where untrusted users or processes can place packets on the network segment.

The switch supports only the active paths method of determining the best return path back to a unicast source address. The active paths method looks up the best reverse path entry in the forwarding table. It does not consider alternate routes specified using routing-protocol-specific methods when determining the best return path.

If the forwarding table lists the receiving interface as the interface to use to forward the packet back to its unicast source, it is the best return path interface.

Use strict mode unicast RPF only on symmetrically routed interfaces. (For information about symmetrically routed interfaces, see [“When to Enable Unicast RPF” on page 154.](#))

For more information about strict unicast RPF, see RFC 3704, *Ingress Filtering for Multihomed Networks* at <http://www.ietf.org/rfc/rfc3704.txt>.

## Unicast RPF Implementation

This section includes:

- [Unicast RPF Packet Filtering on page 154](#)
- [Bootstrap Protocol \(BOOTP\) and DHCP Requests on page 154](#)
- [Default Route Handling on page 154](#)

---

### Unicast RPF Packet Filtering

When you enable unicast RPF on the switch, the switch handles traffic in the following manner:

- If the switch receives a packet on the interface that is the best return path to the unicast source address of that packet, the switch forwards the packet.
- If the best return path from the switch to the packet's unicast source address is not the receiving interface, the switch discards the packet.
- If the switch receives a packet that has a source IP address that does not have a routing entry in the forwarding table, the switch discards the packet.

---

### Bootstrap Protocol (BOOTP) and DHCP Requests

Bootstrap protocol (BOOTP) and DHCP request packets are sent with a broadcast MAC address and therefore the switch does not perform unicast RPF checks on them. The switch forwards all BOOTP packets and DHCP request packets without performing unicast RPF checks.

---

### Default Route Handling

If the best return path to the source is the default route (**0.0.0.0**) and the default route points to **reject**, the switch discards the packets. If the default route points to a valid network interface, the switch performs a normal unicast RPF check on the packets.

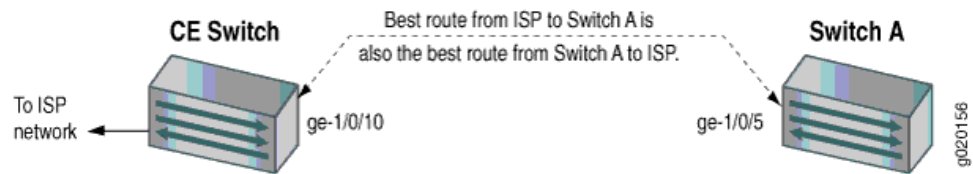
## When to Enable Unicast RPF

Enable unicast RPF when you want to ensure that traffic arriving on a network interface comes from a source that resides on a network that that interface can reach. You can enable unicast RPF on untrusted interfaces to filter spoofed packets. For example, a common application for unicast RPF is to help defend an enterprise network from DoS/DDoS attacks coming from the Internet.

Enable unicast RPF only on symmetrically routed interfaces. A symmetrically routed interface uses the same route in both directions between the source and the destination, as shown in [Figure 9 on page 155](#). Symmetrical routing means that if an interface receives a packet, the switch uses the same interface to send a reply to the packet source (the receiving interface matches the forwarding-table entry for the best return path to the source).



Figure 9: Symmetrically Routed Interfaces



Enabling unicast RPF on asymmetrically routed interfaces (where different interfaces receive a packet and reply to its source) results in packets from legitimate sources being filtered (discarded) because the best return path is not the same interface that received the packet.

The following switch interfaces are most likely to be symmetrically routed and thus are candidates for unicast RPF enabling:

- The service provider edge to a customer
- The customer edge to a service provider
- A single access point out of the network (usually on the network perimeter)
- A terminal network that has only one link



**NOTE:** Because unicast RPF is enabled globally on EX3200, EX4200, EX4300, and EX4500 switches, ensure that *all* interfaces are symmetrically routed before you enable unicast RPF on these switches. Enabling unicast RPF on asymmetrically routed interfaces results in packets from legitimate sources being filtered.



**TIP:** Enabling unicast RPF as close as possible to the traffic source stops spoofed traffic before it can proliferate or reach interfaces that do not have unicast RPF enabled.

## When Not to Enable Unicast RPF

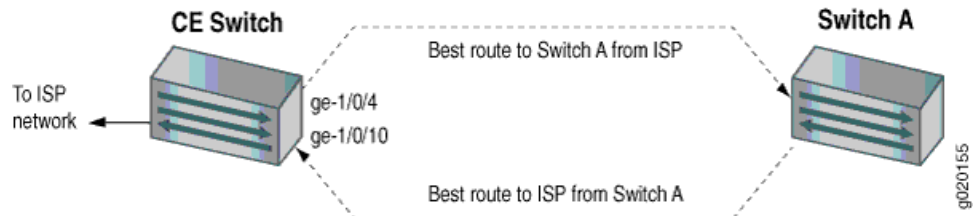
Typically, you will not enable unicast RPF if:

- Switch interfaces are multihomed.
- Switch interfaces are trusted interfaces.
- BGP is carrying prefixes and some of those prefixes are not advertised or are not accepted by the ISP under its policy. (The effect in this case is the same as filtering an interface by using an incomplete access list.)
- Switch interfaces face the network core. Core-facing interfaces are usually asymmetrically routed.

An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination, as shown in [Figure 10 on page 156](#). This means

that if an interface receives a packet, that interface does not match the forwarding table entry as the best return path back to the source. If the receiving interface is not the best return path to the source of a packet, unicast RPF causes the switch to discard the packet even though it comes from a valid source.

Figure 10: Asymmetrically Routed Interfaces



**NOTE:** Do not enable unicast RPF on EX3200, EX4200, EX4300, and EX4500 switches if any switch interfaces are asymmetrically routed, because unicast RPF is enabled globally on all interfaces of these switches. All switch interfaces must be symmetrically routed for you to enable unicast RPF without the risk of the switch discarding traffic that you want to forward.

## Limitations of the Unicast RPF Implementation on EX3200, EX4200, EX4300, and EX4500 Switches

On EX3200, EX4200, EX4300, and EX4500 switches, the switch implements unicast RPF on a global basis. You cannot enable unicast RPF on a per-interface basis. Unicast RPF is globally disabled by default.

- When you enable unicast RPF on any interface, it is automatically enabled on all switch interfaces, including link aggregation groups (LAGs), integrated routing and bridging (IRB) interfaces, and routed VLAN interfaces (RVIs).
- When you disable unicast RPF on the interface (or interfaces) on which you enabled unicast RPF, it is automatically disabled on all switch interfaces.



**NOTE:** You must explicitly disable unicast RPF on every interface on which it was explicitly enabled or unicast RPF remains enabled on all switch interfaces.

QFX switches, OCX switches, and EX3200 and EX4200 switches do not perform unicast RPF filtering on equal-cost multipath (ECMP) traffic. The unicast RPF check examines only one best return path to the packet source, but ECMP traffic employs an address block consisting of multiple paths. Using unicast RPF to filter ECMP traffic on these switches can result in the switch discarding packets that you want to forward because the unicast RPF filter does not examine the entire ECMP address block.

### Related Documentation

- [Example: Configuring Unicast RPF on an EX Series Switch](#)
- [Configuring Unicast RPF \(CLI Procedure\) on page 160](#)

- [Disabling Unicast RPF \(CLI Procedure\) on page 162](#)

## Understanding Unknown Unicast Forwarding

Unknown unicast traffic consists of unicast packets with unknown destination MAC addresses. By default, the switch floods these unicast packets that are traveling in a VLAN to all interfaces that are members of the VLAN. Forwarding this type of traffic can create unnecessary traffic that leads to poor network performance or even a complete loss of network service. This is known as a traffic storm.

To prevent a storm, you can disable the flooding of unknown unicast packets to all VLAN interfaces by configuring one VLAN or all VLANs to forward all unknown unicast traffic to a specific interface. This channels the unknown unicast traffic to a single interface.

### Related Documentation

- [Configuring Unknown Unicast Forwarding \(CLI Procedure\) on page 165](#)
- [Understanding Storm Control on EX Series Switches](#)
- [Understanding Storm Control on Switching Devices](#)
- [Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches](#)

## Example: Configuring Storm Control to Prevent Network Outages

Storm control enables you to prevent network outages caused by broadcast storms on the LAN. You can configure storm control on to rate-limit broadcast traffic, multicast traffic, and unknown unicast traffic at a specified level and to have packets dropped when the specified traffic level is exceeded, thereby preventing packets from proliferating and degrading the LAN.



**NOTE:** This example uses a Junos OS release that supports the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Example: Configuring Storm Control to Prevent Network Outages*.

- [Requirements on page 157](#)
- [Overview and Topology on page 158](#)
- [Configuration on page 158](#)

### Requirements

This example uses the following hardware and software components:

- One QFX Series switch running Junos OS with ELS
- Junos OS Release 13.2 or later

## Overview and Topology

A storm is generated when messages are broadcast on a network and each message prompts a receiving node to respond by broadcasting its own messages on the network. This, in turn, prompts further responses, creating a snowball effect and resulting in a broadcast storm that can cause network outages.

You can use storm control to prevent broadcast storms by specifying the amount, also known as the *storm control level*, of broadcast traffic, multicast traffic, and unknown unicast traffic to be allowed on an interface. You specify the storm control level as the traffic rate in kilobits per second (Kbps) of the combined applicable traffic streams or as the percentage of available bandwidth used by the combined applicable traffic streams. On ELS systems, storm control is enabled by default on all interfaces at a level of 80 percent of the available bandwidth.

Storm control monitors the level of applicable incoming traffic and compares it with the level that you specify. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. As an alternative to having the switch drop packets, you can configure storm control to shut down interfaces or temporarily disable interfaces (see the **action-shutdown** statement or the **recovery-timeout** statement) when the storm control level is exceeded.



**NOTE:** If you configure storm control on an aggregated Ethernet interface, the storm-control level applies to each member interface individually. For example, if the aggregated interface has two members and you configure a storm-control level of 20 kbps, Junos will not detect a storm if one or both of the member interfaces receives traffic at 15 kbps because in neither of these cases does an individual member receive traffic at a rate greater than the configured storm-control level. In this example, Junos detects a storm only if at least one member interface receives traffic at greater than 20 Kbps.

The topology used in this example consists of one switch connected to various network devices. This example shows how to configure the storm control level on interface xe-0/0/0 by setting the level to a traffic rate of 15,000 Kbps, based on the traffic rate of the combined applicable traffic streams. If the combined traffic exceeds this level, the switch drops packets for the controlled traffic types to prevent a network outage.

## Configuration

### CLI Quick Configuration

To quickly configure storm control based on the traffic rate in kilobits per second of the combined traffic streams, copy the following command and paste it into the switch terminal window:

```
[edit]
set forwarding-options storm-control-profiles sc-profile all bandwidth-level 15000
set interfaces xe-0/0/0 unit 0 family ethernet-switching storm-control sc-profile
```

**Step-by-Step Procedure** To configure storm control:

1. Configure a storm control profile, **sc-profile**, and specify the traffic rate in kilobits per second of the combined traffic streams:

```
[edit]
user@switch> set forwarding-options storm-control-profiles sc-profile all bandwidth-level 15000
```

2. Bind the storm control profile, **sc**, to a logical interface:

```
[edit]
user@switch> set interfaces xe-0/0/0 unit 0 family ethernet-switching storm-control sc-profile
```

**Results** Display the results of the configuration:

```
[edit forwarding-options]
user@switch> show storm-control-profiles sc-profile
all {
 bandwidth 15000;
}

[edit]
user@switch> show interfaces xe-0/0/0
unit 0 {
 family ethernet-switching {
 vlan {
 members default;
 }
 storm-control sc-profile;
 }
}
```

- Related Documentation**
- [Understanding Storm Control on page 151](#)
  - [Configuring Autorecovery for MAC Limited or Storm Control Interfaces \(CLI Procedure\)](#)

## Verifying That the Port Error Disable Setting Is Working Correctly

**Purpose** Verify that the port error disable setting is working as expected for MAC limited and storm control interfaces.

**Action** Display information about interfaces:

```
user@switch> show ethernet-switching interfaces
```

| Interface    | State | VLAN members | Blocking                |
|--------------|-------|--------------|-------------------------|
| xe-2:0/0/0.0 | up    | T1122        | unblocked               |
| xe-2:0/0/1.0 | down  | default      | MAC limit exceeded      |
| xe-2:0/0/2.0 | down  | default      | Storm control in effect |
| xe-2:0/0/3.0 | down  | default      | unblocked               |
| xe-2:0/0/4.0 | down  | default      | unblocked               |
| xe-2:0/0/5.0 | down  | default      | unblocked               |
| xe-2:0/0/6.0 | down  | default      | unblocked               |

**Meaning** For interfaces disabled by port security features, the sample output from the **show ethernet-switching interfaces** command specifies the reasons that the interfaces are disabled:

- **MAC limit exceeded**—The interface is temporarily disabled because of a *mac-limit* error. The disabled interface is automatically restored to service when the *disable-timeout* (*Port Error Disable*) expires.
- **MAC move limit exceeded**—The interface is temporarily disabled because of a *mac-move-limit* error. The disabled interface is automatically restored to service when the *disable-timeout* expires.
- **Storm control in effect**—The interface is temporarily disabled because of a *storm-control* error. The disabled interface is automatically restored to service when the *disable-timeout* (*Port Error Disable*) expires.

- Related Documentation**
- [Understanding MAC Limiting and MAC Move Limiting for Port Security on page 135](#)
  - [port-error-disable on page 252](#)
  - [Configuring Autorecovery for MAC Limited or Storm Control Interfaces \(CLI Procedure\)](#)

## Configuring Unicast RPF (CLI Procedure)

Unicast reverse-path forwarding (RPF) can help protect your LAN from denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks on untrusted interfaces. Enabling unicast RPF on the switch interfaces filters traffic with source addresses that do not use the incoming interface as the best return path back to the source. When a packet comes into an interface, if that interface is not the best return path to the source, the switch discards the packet. If the incoming interface is the best return path to the source, the switch forwards the packet.



**NOTE:** On EX3200, EX4200, and EX4300 switches, you can enable unicast RPF only globally—that is, on all switch interfaces. You cannot enable unicast RPF on a per-interface basis.

Before you begin:

- On an EX8200, EX6200, QFX Series switch, or OCX Series switch, ensure that the selected switch interface is symmetrically routed before you enable unicast RPF. A symmetrically routed interface is an interface that uses the same route in both directions between the source and the destination. Do not enable unicast RPF on asymmetrically routed interfaces. An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination.
- On an EX3200, EX4200, or EX4300 switch, ensure that *all* switch interfaces are symmetrically routed before you enable unicast RPF on an interface. When you enable unicast RPF on any interface, it is enabled globally on all switch interfaces. Do not enable unicast RPF on asymmetrically routed interfaces. An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination.

To enable unicast RPF, configure it explicitly on a selected customer-edge interface:

[edit interfaces]

user@switch# **set ge-1/0/10 unit 0 family inet rpf-check**



**BEST PRACTICE:** On EX3200, EX4200, and EX4300 switches, unicast RPF is enabled globally on *all* switch interfaces, regardless of whether you configure it explicitly on only one interface or only on some interfaces.

On EX3200, EX4200, and EX4300 switches, we recommend that you enable unicast RPF explicitly on either all interfaces or only one interface. To avoid possible confusion, do not enable it on only some interfaces:

- Enabling unicast RPF explicitly on only one interface makes it easier if you choose to disable it in the future because you must explicitly disable unicast RPF on every interface on which you explicitly enabled it. If you explicitly enable unicast RPF on two interfaces and you disable it on only one interface, unicast RPF is still implicitly enabled globally on the switch. The drawback of this approach is that the switch displays the flag that indicates that unicast RPF is enabled only on interfaces on which unicast RPF is explicitly enabled, so even though unicast RPF is enabled on all interfaces, this status is not displayed.
- Enabling unicast RPF explicitly on all interfaces makes it easier to know whether unicast RPF is enabled on the switch because every interface shows the correct status. (Only interfaces on which you explicitly enable unicast RPF display the flag that indicates that unicast RPF is enabled.) The drawback of this approach is that if you want to disable unicast RPF, you must explicitly disable it on every interface. If unicast RPF is enabled on any interface, it is implicitly enabled on all interfaces.

#### Related Documentation

- *Example: Configuring Unicast RPF on an EX Series Switch*
- [Verifying Unicast RPF Status on page 162](#)
- [Disabling Unicast RPF \(CLI Procedure\) on page 162](#)

- [Troubleshooting Unicast RPF](#)
- [Understanding Unicast RPF on page 153](#)

## Disabling Unicast RPF (CLI Procedure)

---

Unicast reverse-path forwarding (RPF) can help protect your LAN from denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks on untrusted interfaces. Unicast RPF filters traffic with source addresses that do not use the incoming interface as the best return path back to the source. If the network configuration changes so that an interface that has unicast RPF enabled becomes a trusted interface or becomes asymmetrically routed (the interface that receives a packet is not the best return path to the packet's source), disable unicast RPF.

To disable unicast RPF on an EX3200, EX4200, or EX4300 switch, you must delete it from every interface on which you explicitly configured it. If you do not disable unicast RPF on every interface on which you explicitly enabled it, it remains implicitly enabled on all interfaces. If you attempt to delete unicast RPF from an interface on which it was not explicitly enabled, the **warning: statement not found** message appears. If you do not disable unicast RPF on every interface on which you explicitly enabled it, unicast RPF remains implicitly enabled on all interfaces of the EX3200, EX4200, or EX4300 switch.

On EX8200, EX6200, QFX Series switches, and OCX Series switches, the switch does not apply unicast RPF to an interface unless you explicitly enable that interface for unicast RPF.

To disable unicast RPF, delete its configuration from the interface:

[edit interfaces]

user@switch# **delete** ge-1/0/10 unit 0 family inet **rpf-check**



**NOTE:** On EX3200, EX4200, and EX4300 switches, if you do not disable unicast RPF on every interface on which you explicitly enabled it, unicast RPF remains implicitly enabled on all interfaces.

### Related Documentation

- [Example: Configuring Unicast RPF on an EX Series Switch](#)
- [Verifying Unicast RPF Status on page 162](#)
- [Configuring Unicast RPF \(CLI Procedure\) on page 160](#)
- [Understanding Unicast RPF on page 153](#)

## Verifying Unicast RPF Status

---

**Purpose** Verify that unicast reverse-path forwarding (RPF) is enabled and is working on the interface.



**Action** Use one of the **show interfaces *interface-name*** commands with either the **extensive** or **detail** options to verify that unicast RPF is enabled and working on the switch. The following example displays output from the **show interfaces ge- extensive** command.

```

user@switch> show interfaces ge-1/0/10 extensive
Physical interface: ge-1/0/10, Enabled, Physical link is Down
 Interface index: 139, SNMP ifIndex: 58, Generation: 140
 Link-level type: Ethernet, MTU: 1514, Speed: Auto, MAC-REWRITE Error: None,
 Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled,
 Auto-negotiation: Enabled, Remote fault: Online
 Device flags : Present Running
 Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
 Link flags : None
 CoS queues : 8 supported, 8 maximum usable queues
 Hold-times : Up 0 ms, Down 0 ms
 Current address: 00:19:e2:50:95:ab, Hardware address: 00:19:e2:50:95:ab
 Last flapped : Never
 Statistics last cleared: Never
 Traffic statistics:
 Input bytes : 0 0 bps
 Output bytes : 0 0 bps
 Input packets: 0 0 pps
 Output packets: 0 0 pps
 IPv6 transit statistics:
 Input bytes : 0
 Output bytes : 0
 Input packets: 0
 Output packets: 0
 Input errors:
 Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
 L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
 FIFO errors: 0, Resource errors: 0
 Output errors:
 Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,

 FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
 Egress queues: 8 supported, 4 in use
 Queue counters: Queued packets Transmitted packets Dropped packets

 0 best-effort 0 0 0
 1 assured-forw 0 0 0
 5 expedited-fo 0 0 0
 7 network-cont 0 0 0

 Active alarms : LINK
 Active defects : LINK
 MAC statistics:
 Receive Transmit
 Total octets 0 0
 Total packets 0 0
 Unicast packets 0 0
 Broadcast packets 0 0
 Multicast packets 0 0
 CRC/Align errors 0 0
 FIFO errors 0 0
 MAC control frames 0 0
 MAC pause frames 0 0
 Oversized frames 0 0
 Jabber frames 0 0

```

```

Fragment frames 0
VLAN tagged frames 0
Code violations 0
Filter statistics:
Input packet count 0
Input packet rejects 0
Input DA rejects 0
Input SA rejects 0
Output packet count 0
Output packet pad count 0
Output packet error count 0
CAM destination filters: 0, CAM source filters: 0
Autonegotiation information:
Negotiation status: Incomplete
Packet Forwarding Engine configuration:
Destination slot: 1

Logical interface ge-1/0/10.0 (Index 69) (SNMP ifIndex 59) (Generation 135)
Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Protocol inet, Generation: 144, Route table: 0
Flags: uRPF
Addresses, Flags: Is-Preferred Is-Primary

```

**Meaning** The `show interfaces ge-1/0/10 extensive` command (and the `show interfaces ge-1/0/10 detail` command) displays in-depth information about the interface. The **Flags:** output field near the bottom of the display reports the unicast RPF status. If unicast RPF has not been enabled, the **uRPF** flag is not displayed.

On EX3200, EX4200, and EX4300 switches, unicast RPF is implicitly enabled on *all* switch interfaces, including aggregated Ethernet interfaces (also referred to as link aggregation groups or LAGs), integrated routing and bridging (IRB) interfaces, and routed VLAN interfaces (RVIs) when you enable unicast RPF on a single interface. However, the unicast RPF status is shown as enabled only on interfaces for which you have explicitly configured unicast RPF. Thus, the **uRPF** flag is not displayed on interfaces for which you

have not explicitly configured unicast RPF even though unicast RPF is implicitly enabled on all interfaces on EX3200 and EX4200 switches.

**Related  
Documentation**

- *show interfaces xe-*
- *Example: Configuring Unicast RPF on an EX Series Switch*
- [Configuring Unicast RPF \(CLI Procedure\) on page 160](#)
- [Disabling Unicast RPF \(CLI Procedure\) on page 162](#)
- *Troubleshooting Unicast RPF*

## Configuring Unknown Unicast Forwarding (CLI Procedure)



**NOTE:** This task uses Junos OS for EX Series switches or QFX Series with support for the Enhanced Layer 2 Software (ELS) configuration style. If your EX Series switch runs software that does not support ELS, see *Configuring Unknown Unicast Forwarding (CLI Procedure)*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*

Unknown unicast traffic consists of packets with unknown destination MAC addresses. By default, the switch floods these packets to all interfaces associated with a VLAN. Forwarding such traffic to interfaces on the switch can create a security issue.

To prevent flooding unknown unicast traffic across the switch, configure unknown unicast forwarding to direct all unknown unicast packets within a VLAN out to a specific interface. You can configure each VLAN to divert unknown unicast traffic to different interfaces or use one interface for multiple VLANs.

To configure unknown unicast forwarding options:

- Configure unknown unicast forwarding for a specific VLAN (here, the VLAN name is employee), and specify the interface to which all unknown unicast traffic will be forwarded:

```
[edit switch-options]
user@switch# set unknown-unicast-forwarding vlan vlan-name interface ge-x/y/z.0
```

**Related  
Documentation**

- *Verifying That Unknown Unicast Packets Are Forwarded to a Single Interface*
- [Understanding Unknown Unicast Forwarding on page 157](#)



## PART 6

# Using DDOS Protection

- [Overview of DDOS Protection on page 169](#)
- [Configuring DDOS Protection on page 171](#)
- [Monitoring DDOS Protection on page 181](#)



## CHAPTER 6

# Overview of DDOS Protection

- [Understanding Distributed Denial-of-Service Protection on QFX Series Switches on page 169](#)

## Understanding Distributed Denial-of-Service Protection on QFX Series Switches

---

A denial-of-service (DoS) attack is any attempt to deny valid users access to network or server resources by using up all the resources of the network element or server. Distributed denial-of-service attacks (DDoS) involve an attack from multiple sources, enabling a much greater amount of traffic to attack the network. The attacks typically use network protocol control packets to trigger a large number of exceptions to the router or switch control plane. This results in an excessive processing load that disrupts normal network operations.

Junos OS DDoS protection enables switches to continue functioning while under attack. It identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed. A single point of DDoS protection management enables network administrators to customize profiles for their network control traffic.

To protect against DDoS attacks, you can configure policers for host-bound exception traffic. The policers specify rate limits for all control traffic for a given protocol, or, in some cases, for specific control packet types for a protocol. Control traffic is dropped when it exceeds any configured policer values or, for unconfigured policers, the default policer values. Each violation immediately generates a notification to alert operators about a possible attack. The violation is counted, the time that the violation starts is noted, and the time of the last observed violation is noted. When the traffic rate drops below the bandwidth violation threshold, a recovery timer determines when the traffic flow is considered to have returned to normal. If no further violation occurs before the timer expires, the violation state is cleared and a notification is generated. On QFX Series switches, the timer is set to 300 seconds and cannot be modified.

In addition to providing notification of violations through event logging, Junos OS DDoS protection allows you to monitor policers, obtaining information such as the policer configuration, number of violations encountered, date and time of violations, packet arrival rates, and number of packets received or dropped.

## Policer Enforcement Points on QFX Series Switches

On switches, control traffic arriving from all ports of the switch converges on the Packet Forwarding Engine, where it is subject to policing. Thus, excess packets are dropped before they reach the Routing Engine, ensuring that the Routing Engine receives only the amount of traffic it can process.

- Related Documentation**
- [Configuring DDoS Protection Policers on QFX Series Switches on page 174](#)
  - [Verifying and Managing DDoS Protection on page 181](#)



## CHAPTER 7

# Configuring DDOS Protection

- [Example: Configuring DDoS Protection on QFX Series Switches on page 171](#)
- [Disabling DDoS Protection Policers and Logging Globally on page 174](#)
- [Configuring DDoS Protection Policers on QFX Series Switches on page 174](#)
- [Tracing DDoS Protection Operations on page 177](#)

### Example: Configuring DDoS Protection on QFX Series Switches

---

This example shows how to configure DDoS protection that enables a switch to quickly identify an attack and prevent a flood of malicious control packets from exhausting system resources.

- [Requirements on page 171](#)
- [Overview on page 171](#)
- [Configuration on page 172](#)
- [Verification on page 173](#)

### Requirements

DDoS protection requires the following hardware and software:

- QFX Series switch that supports DDoS protection
- Junos OS Release 14.1X53-D40 or later

No special configuration beyond device initialization is required before you can configure this feature.

### Overview

Distributed denial-of-service (DDoS) attacks use multiple sources to flood a network with protocol control packets. This malicious traffic triggers a large number of exceptions in the network and attempts to exhaust the system resources to deny valid users access to the network or server.

DDoS protection is enabled by default on a supported QFX Series switch. This example describes how you can modify the default configuration for the rate-limiting policers that identify excess control traffic and drop the packets before the switch is adversely affected.

Sample tasks include configuring an aggregate policer for a protocol group and specifying trace options for DDoS operations.

This example does not show all possible configuration choices.

## Configuration

**CLI Quick Configuration** To quickly configure DDoS protection for protocol groups and particular control packet types, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

```
[edit]
edit system
set ddos-protection protocols isis aggregate bandwidth 150
set ddos-protection protocols isis aggregate burst 2000
set ddos-protection traceoptions file ddos-trace size 10m
set ddos-protection traceoptions flag all
top
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure DDoS protection:

1. Specify a protocol group.  

```
[edit system ddos-protection protocols]
user@host# edit isis
```
2. Configure the maximum traffic rate for the RADIUS aggregate policer; that is, for the combination of all RADIUS packets.  

```
[edit system ddos-protection protocols isis]
user@host# set aggregate bandwidth 150
```
3. Configure the maximum burst rate for the RADIUS aggregate policer.  

```
[edit system ddos-protection protocols isis]
user@host# set aggregate burst 2000
```
4. Configure tracing for all DDoS protocol processing events.  

```
[edit system ddos-protection traceoptions]
user@host# set file ddos-log
user@host# set file size 10m
user@host# set flag all
```

**Results** From configuration mode, confirm your configuration by entering the **show ddos-protection** command at the **system** hierarchy level.

```
[edit system]

user@host# show ddos-protection

traceoptions {
```

```

 file ddos-log size 10m;
 flag all;
 }
 protocols {
 isis {
 aggregate {
 bandwidth 150;
 burst 2000;
 }
 }
 }
}

```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

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

- [Verifying the DDoS Protection Configuration on page 173](#)

### Verifying the DDoS Protection Configuration

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>               | Verify that the RADIUS policer values have changed from the default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Action</b>                | <p>From operational mode, enter the <b>show ddos-protection protocols isis parameters</b> command.</p> <pre> user@host&gt; show ddos-protection protocols isis parameters Packet types: 5, Modified: 3 * = User configured value  Protocol Group: ISIS  Packet type: aggregate (Aggregate for all ISIS traffic) Aggregate policer configuration:   Bandwidth:      150 pps*   Burst:          2000 packets*   Recover time:   300 seconds   Enabled:        Yes Routing Engine information:   Bandwidth: 150 pps, Burst: 2000 packets, enabled FPC slot 0 information:   Bandwidth: 100% (150 pps), Burst: 100% (2000 packets), enabled </pre> |
| <b>Meaning</b>               | The command output shows the current configuration of the ISIS aggregate policer. Policer values that have been modified from the default values are marked with an asterisk. The output shows that the RADIUS policer configuration has been modified correctly.                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b> | <ul style="list-style-type: none"> <li>• <a href="#">Understanding Distributed Denial-of-Service Protection on QFX Series Switches on page 169</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

- [Configuring DDoS Protection Policers on QFX Series Switches on page 174](#)

## Disabling DDoS Protection Policers and Logging Globally

---

DDoS policers are enabled by default for all supported protocol groups and packet types. Policers are established at the level of the individual line card and the Routing Engine. You can disable the line card policers globally for all MPCs or FPC5s. You can also disable the Routing Engine policer. When you disable either of these policers, the policers at that level for all protocol groups and packet types are disabled.



**NOTE:** On QFX5100 switches, DDoS policers are enabled by default for all supported protocol groups, at the level of the switch.

DDoS logging is also enabled by default. You can disable all DDoS event logging (including flow detection event logging) for all protocol groups and packet types across the router. You can disable DDoS event logging for all protocol groups across the switch.



**NOTE:** The global configuration for disabling policers and logging overrides any local configuration for packet types.

Packet-type policers are not supported on QFX5100 switches.

To configure global DDoS settings:

1. (Optional) Disable line card or switch policers.

```
[edit system ddos-protection global]
user@host# set disable-fpc
```

2. (Optional) Disable Routing Engine policers (not supported on QFX5100 switches).

```
[edit system ddos-protection global]
user@host# set disable-routing-engine
```

3. (Optional) Disable event logging.

```
[edit system ddos-protection global]
user@host# set disable-logging
```

### Related Documentation

- [Configuring Protection Against DDoS Attacks](#)
- [Configuring DDoS Protection Policers on QFX Series Switches on page 174](#)

## Configuring DDoS Protection Policers on QFX Series Switches

---

You can modify the DDoS protection configuration as follows:

- Modify the aggregate policer bandwidth and burst values for a protocol group. Default values exist for all protocol groups. See [protocols](#) for the supported protocol groups and their default policer values.
- Scale the bandwidth and burst values for a policer on the switch so that the policer triggers at lower thresholds than the overall protocol thresholds.
- Disable logging for a specific policer.
- Disable a policer on the switch (the “FPC”). This action is effectively the same as disabling the policers globally. Note that deleting the configuration for a policer does not disable it—the policer merely reverts to its default settings.



**BEST PRACTICE:** We recommend that you model your network to determine the best values for your situation. Before you configure policers for your network, you can quickly view the default values for all protocol groups and packet types from operational mode by issuing the [show ddos-protection protocols parameters brief](#) command. You can also use the command to specify a single protocol group of interest; for example, issue the [show ddos-protection protocols radius parameters brief](#) command.

This topic describes:

- [Configuring the Aggregate Policer for a Protocol Group on page 175](#)
- [Configuring Policers' Bandwidth and Burst Values on the Switch on page 176](#)
- [Disabling Policers and Policer Logging on page 176](#)

## Configuring the Aggregate Policer for a Protocol Group

An aggregate policer exists for each protocol group. The aggregate policer enforces the traffic limits on the control packets for that protocol as a combined group.

To configure the DDoS aggregate policer for a protocol group:

1. Specify the aggregate policer for the protocol group.

```
[edit system ddos-protection protocols]
user@host# edit protocol-group aggregate
```

For example, to specify the DHCPv4v6 aggregate policer:

```
[edit system ddos-protection protocols]
user@host# edit dhcpv4v6 aggregate
```

2. (Optional) Configure the maximum traffic rate the policer allows for the protocol group.

```
[edit system ddos-protection protocols protocol-group aggregate]
user@host# set bandwidth packets-per-second
```

For example, to set a bandwidth of 300 packets per second for DHCPv4 and DHCPv6 packets:

```
[edit system ddos-protection protocols dhcpv4v6 aggregate]
```

```
user@host# set bandwidth 300
```

3. (Optional) Configure the maximum number of packets that the policer allows in a burst of traffic.

```
[edit system ddos-protection protocols protocol-group aggregate]
user@host# set burst size
```

For example, to set a maximum of 1500 DHCPv4v6 packets:

```
[edit system ddos-protection protocols dhcpv4v6 aggregate]
user@host# set burst 1500
```

## Configuring Policers' Bandwidth and Burst Values on the Switch

You can alter a policer behavior on the switch by scaling the policer's configured bandwidth and burst values.

- To scale the maximum bandwidth for a policer:

```
[edit system ddos-protection protocols protocol-group aggregate]
user@host# set fpc slot-number bandwidth-scale percentage
```

For example, to scale the maximum bandwidth allowed by the DHCPv4v6 aggregate policer for the FPC or line card to 80 percent:

```
[edit system ddos-protection protocols dhcpv4v6 aggregate]
user@host# set fpc 0 bandwidth-scale 80
```

- To scale the maximum burst size for a policer:

```
[edit system ddos-protection protocols protocol-group aggregate]
user@host# set fpc slot-number burst-scale percentage
```

For example, to scale the maximum burst size to 75 percent for OSPF on the FPC (in this case, on a Virtual Chassis member) in slot 1:

```
[edit system ddos-protection protocols ospf]
user@host# set fpc 1 burst-scale 75
```

## Disabling Policers and Policer Logging

All supported policers are enabled by default. You can disable specific policers on the switch. Similarly, event logging by policers is enabled by default. You can selectively disable logging by a policer.

- To disable a policer on a specific member of a Virtual Chassis:

```
[edit system ddos-protection protocols]
user@host# set protocol-groupaggregate fpc slot-number disable-fpc
```

For example, to disable the DDoS policers for DHCP on member 3:

```
[edit system ddos-protection protocols]
user@host# set dhcp fpc 3 disable-fpc
```

- To disable a policer on the switch or on all members of the Virtual Chassis:

```
[edit system ddos-protection protocols]
user@host# set protocol-groupaggregate disable-fpc
```

For example, to disable the aggregate policer for the BFD protocol group on the switch:

```
[edit system ddos-protection protocols]
user@host# set bfd aggregate disable-fpc
```

- To disable event logging by a policer:

```
[edit system ddos-protection protocols]
user@host# set protocol-group aggregate disable-logging
```

For example, to disable logging by the aggregate BFD policer:

```
[edit system ddos-protection protocols]
user@host# set bfd aggregate disable-logging
```

#### Related Documentation

- [Example: Configuring DDoS Protection on QFX Series Switches on page 171](#)

## Tracing DDoS Protection Operations

The Junos OS trace feature tracks DDoS protection operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file located in the `/var/log` directory. By default, the router uses the filename `jddosd`. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file *filename* reaches 128 kilobytes (KB), it is compressed and renamed *filename.0.gz*. Subsequent events are logged in a new file called *filename*, until it reaches capacity again. At this point, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

You can optionally specify the number of trace files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB). (For more information about how log files are created, see the [System Log Explorer](#).)

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

This topic describes how you can configure all aspects of DDoS tracing operations. It covers:

- [Configuring the DDoS Protection Trace Log Filename on page 178](#)
- [Configuring the Number and Size of DDoS Protection Log Files on page 178](#)
- [Configuring Access to the DDoS Protection Log File on page 178](#)
- [Configuring a Regular Expression for DDoS Protection Messages to Be Logged on page 179](#)

- [Configuring the DDoS Protection Tracing Flags on page 179](#)
- [Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged on page 179](#)

## Configuring the DDoS Protection Trace Log Filename

By default, the name of the file that records trace output for DDoS protection is **ddosd**. You can specify a different name with the **file** option.

To configure the filename for subscriber management database tracing operations:

- Specify the name of the file used for the trace output.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos_logfile_1
```

## Configuring the Number and Size of DDoS Protection Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format **.number.gz**. The newest archived file is **.0.gz** and the oldest archived file is **.(maximum number)-1.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can 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 compressed and renamed **filename.0.gz**, and a new file called **filename** is created. When the new **filename** reaches 2 MB, **filename.0.gz** is renamed **filename.1.gz** and **filename** is compressed and renamed **filename.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, **filename.19.gz**, is simply overwritten when the next oldest file, **filename.18.gz** is compressed and renamed to **filename.19.gz**.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos_1_logfile_1 files 20 size 2097152
```

## Configuring Access to the DDoS Protection Log File

By default, only the user who configures the tracing operation can access the log files. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable.

```
[edit system ddos-protection traceoptions]
```



```
user@host# set file ddos_1_logfile_1 world-readable
```

To explicitly set the default behavior, only the user who configured tracing can read the log file:

- Configure the log file to be no-world-readable.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos_1_logfile_1 no-world-readable
```

## Configuring a Regular Expression for DDoS Protection Messages to Be Logged

By default, the trace operation output includes all messages relevant to the logged events.

You can refine the output by including regular expressions to be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos_1_logfile_1 match regex
```

## Configuring the DDoS Protection Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit system ddos-protection traceoptions]
user@host# set flag flag
```

## Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged

The messages associated with a logged event are categorized according to severity level. You can use the severity level to determine which messages are logged for the event type. The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **all** or **verbose**. Either choice generates a large amount of output. You can specify a more restrictive severity level, such as **notice** or **info** to filter the messages. By default, the trace operation output includes only messages with a severity level of **error**.

To configure the type of messages to be logged:

- Configure the message severity level.

```
[edit system ddos-protection traceoptions]
user@host# set level severity
```

- Related Documentation**
- *Configuring Protection Against DDoS Attacks*
  - [Configuring DDoS Protection Policers on QFX Series Switches on page 174](#)

# Monitoring DDoS Protection

- [Verifying and Managing DDoS Protection on page 181](#)

## Verifying and Managing DDoS Protection

---

- Purpose** View or clear information about DDoS configurations, states, and statistics.
- Action**
- To display the DDoS policer configuration, violation state, and statistics for all packet types in all protocol groups:  
`user@host> show ddos-protection protocols`  
If you issue the command before you make any configuration changes, the default policer values are displayed.
  - To display the DDoS policer configuration, violation state, and statistics for a particular packet type in a particular protocol group:  
`user@host> show ddos-protection protocols protocol-group packet-type`
  - To display only the number of DDoS policer violations for all protocol groups:  
`user@host> show ddos-protection protocols violations`
  - To display a table of the DDoS configuration for all packet types in all protocol groups:  
`user@host> show ddos-protection protocols parameters brief`
  - To display a complete list of packet statistics and DDoS violation statistics for all packet types in all protocol groups:  
`user@host> show ddos-protection protocols statistics detail`
  - To display global DDoS violation statistics:  
`user@host> show ddos-protection statistics`
  - To display the DDoS version number:  
`user@host> show ddos-protection version`
  - To clear DDoS statistics for all packet types in all protocol groups:  
`user@host> clear ddos-protection protocols statistics`
  - To clear DDoS statistics for all packet types in a particular protocol group:  
`user@host> clear ddos-protection protocols protocol-group statistics`

- To clear DDoS statistics for a particular packet type in a particular protocol group:

```
user@host> clear ddos-protection protocols protocol-group statisticspacket-type
```

- To clear DDoS violation states for all packet types in all protocol groups:

```
user@host> clear ddos-protection protocols states
```

- To clear DDoS violation states for all packet types in a particular protocol group:

```
user@host> clear ddos-protection protocols protocol-group states
```

- To clear DDoS violation states for a particular packet type in a particular protocol group:

```
user@host> clear ddos-protection protocols protocol-group statespacket-type
```

**Related  
Documentation**

- *Verifying and Managing Flow Detection*
- [Configuring DDoS Protection Policers on QFX Series Switches on page 174](#)

## PART 7

# Configuration Statements and Operational Commands

- Configuration Statements for Firewall Filters on page 185
- Configuration Statements for Policers on page 195
- Configuration Statements for MACsec on page 215
- Configuration Statements for Port Security on page 243
- Configuration Statements for Device Security on page 257
- Configuration Statements for DDoS Protection on page 269
- Firewall Operational Commands on page 287
- MACsec Operational Commands on page 299
- Port Security Operational Commands on page 311
- DDoS Protection Operational Commands on page 317



## CHAPTER 9

# Configuration Statements for Firewall Filters

- [family on page 186](#)
- [filter on page 187](#)
- [filter \(Layer 2 and Layer 3 Interfaces\) on page 188](#)
- [filter \(VLANs\) on page 189](#)
- [firewall on page 190](#)
- [from on page 191](#)
- [interface-specific on page 192](#)
- [term on page 193](#)
- [then \(Filters\) on page 194](#)

## family

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>family <i>family-name</i> {<br/>    filter <i>filter-name</i> {<br/>        interface-specific;<br/>        term <i>term-name</i> {<br/>            from {<br/>                match-conditions;<br/>            }<br/>            then {<br/>                action;<br/>                action-modifiers;<br/>            }<br/>        }<br/>    }<br/>}</pre>                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit <a href="#">firewall</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | Configure the fields a firewall filter can match on.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <p><i>family-name</i>—Type of addressing protocol:</p> <ul style="list-style-type: none"><li>• <b>ethernet-switching</b>—Filter Layer 2 Ethernet packets and Layer 3 (IP) packets (allows some Layer 3 filtering). Not supported on OCX series switches.</li><li>• <b>inet</b>—Filter Layer 3 IPv4 packets (provides additional Layer 3 filter options).</li><li>• <b>inet6</b>—Filter Layer 3 IPv6 packets (provides additional Layer 3 filter options).</li><li>• <b>mpls</b>—Filter multiprotocol label switched packets. Not supported on OCX series switches.</li></ul> <p>The remaining statements are explained separately.</p> |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Firewall Filter Match Conditions and Actions on page 15</a></li><li>• <a href="#">Configuring Firewall Filters on page 39</a></li><li>• <a href="#">Overview of Firewall Filters on page 3</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                           |



## filter

|                                 |                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> filter <i>filter-name</i> {     <i>interface-specific</i>;     term <i>term-name</i> {         from {             <i>match-conditions</i>;         }         then {             <i>action</i>;             <i>action-modifiers</i>;         }     } } </pre>                     |
| <b>Hierarchy Level</b>          | [edit <b>firewall family</b> <i>family-name</i> ]                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                          |
| <b>Description</b>              | Configure firewall filters.                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <p><b><i>filter-name</i></b>—Name that identifies the filter. The name can contain letters, numbers, and hyphens (-), and can be up to 64 characters long. To include spaces in the name, enclose it in quotation marks.</p> <p>The remaining statements are explained separately.</p> |
| <b>Required Privilege Level</b> | <p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Firewall Filter Match Conditions and Actions on page 15</a></li> <li>• <a href="#">Configuring Firewall Filters on page 39</a></li> <li>• <a href="#">Overview of Firewall Filters on page 3</a></li> </ul>                       |

## filter (Layer 2 and Layer 3 Interfaces)

---

|                                 |                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | filter (input   output) <i>filter-name</i> ;                                                                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> <b>family</b> <i>family-name</i> ]                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | Apply a firewall filter to traffic transiting a port or Layer 3 interface.                                                                                                                                                                                                                                                                |
| <b>Default</b>                  | All incoming traffic is accepted unmodified on the port or Layer 3 interface, and all outgoing traffic is sent unmodified from the port or Layer 3 interface.                                                                                                                                                                             |
| <b>Options</b>                  | <p><b><i>filter-name</i></b>—Name of a firewall filter defined at the [edit firewall family <i>family-name</i> filter] hierarchy level.</p> <p><b>input</b>—Apply a firewall filter to traffic entering the port or Layer 3 interface.</p> <p><b>output</b>—Apply a firewall filter to traffic exiting the port or Layer 3 interface.</p> |
| <b>Required Privilege Level</b> | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Gigabit Ethernet Interfaces (CLI Procedure)</a></li><li>• <a href="#">Configuring Firewall Filters on page 39</a></li><li>• <a href="#">Overview of Firewall Filters on page 3</a></li></ul>                                                                              |

## filter (VLANs)

---

|                                 |                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>filter (input   output) <i>filter-name</i>;</code>                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | <code>[edit vlans <i>vlan-name</i>]</code><br><code>[edit vlans <i>vlan-name</i> forwarding-options]</code>                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                                                                                  |
| <b>Description</b>              | Apply a firewall filter to traffic ingressing or egressing a VLAN.                                                                                                                                                                                                                                 |
| <b>Default</b>                  | All incoming traffic is accepted unmodified to a VLAN, and all outgoing traffic is sent unmodified from a VLAN.                                                                                                                                                                                    |
| <b>Options</b>                  | <p><b><i>filter-name</i></b>—Name of a firewall filter defined at the <code>[edit firewall family <i>family-name</i> filter]</code> hierarchy level.</p> <p><b>input</b>—Apply a firewall filter to VLAN ingress traffic.</p> <p><b>output</b>—Apply a firewall filter to VLAN egress traffic.</p> |
| <b>Required Privilege Level</b> | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Firewall Filters on page 39</a></li> <li>• <a href="#">Overview of Firewall Filters on page 3</a></li> </ul>                                                                                                                      |

## firewall

```

Syntax firewall {
 family family-name {
 filter filter-name {
 interface-specific;
 term term-name {
 from {
 match-conditions;
 }
 then {
 action;
 action-modifiers;
 }
 }
 }
 }
 policer policer-name {
 filter-specific;
 if-exceeding {
 bandwidth-limit bps;
 burst-size-limit bytes;
 }
 then {
 policer-action;
 }
 }
 three-color-policer policer-name {
 action {
 loss-priority high then discard;
 }
 single-rate {
 (color-aware | color-blind);
 committed-information-rate bps;
 committed-burst-size bytes;
 excess-burst-size bytes;
 }
 two-rate {
 (color-aware | color-blind);
 committed-information-rate bps;
 committed-burst-size bytes;
 peak-information-rate bps;
 peak-burst-size bytes;
 }
 }
 }

```

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 firewall filters and policers.

The remaining statements are explained separately.

|                                 |                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Firewall Filter Match Conditions and Actions on page 15</a></li> <li>• <a href="#">Configuring Firewall Filters on page 39</a></li> <li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li> <li>• <a href="#">Overview of Firewall Filters on page 3</a></li> </ul> |

## from

|                                 |                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>from {     match-conditions; }</pre>                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit <b>firewall family</b> <i>family-name</i> <b>filter</b> <i>filter-name</i> <b>term</b> <i>term-name</i> ]                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                |
| <b>Description</b>              | Match packet fields to values specified in a match condition. If the <b>from</b> statement is not included in a firewall filter configuration, all packets are considered to match and the actions and action modifiers in the <b>then</b> statement are implemented.                                                        |
| <b>Options</b>                  | <b>match-conditions</b> —Conditions that define the values or fields that the incoming or outgoing packets must contain for a match. You can specify one or more match conditions. If you specify more than one, they all must match for a match to occur and for the action in the <b>then</b> statement to be implemented. |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Firewall Filter Match Conditions and Actions on page 15</a></li> <li>• <a href="#">Configuring Firewall Filters on page 39</a></li> <li>• <a href="#">Understanding Firewall Filter Match Conditions on page 11</a></li> </ul>                                          |

## interface-specific

---

|                                 |                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | interface-specific;                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit <b>firewall</b> <b>family</b> <i>family-name</i> <b>filter</b> <i>filter-name</i> ]                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                |
| <b>Description</b>              | Configure separate counters for each interface to which a filter is applied.                                                                                                                                                                                 |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Firewall Filter Match Conditions and Actions on page 15</a></li><li>• <a href="#">Configuring Firewall Filters on page 39</a></li><li>• <a href="#">Overview of Firewall Filters on page 3</a></li></ul> |

## term

---

|                                 |                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>term <i>term-name</i> {     from {         <i>match-conditions</i>;     }     then {         <i>action</i>;         <i>action-modifiers</i>;     } }</pre>                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit <b>firewall family</b> <i>family-name</i> <b>filter</b> <i>filter-name</i> ]                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                      |
| <b>Description</b>              | Define a firewall filter term.                                                                                                                                                                                                                                                     |
| <b>Options</b>                  | <p><b><i>term-name</i></b>—Name that identifies the term. The name can contain letters, numbers, and hyphens (-), and can be up to 64 characters long. To include spaces in the name, enclose it in quotation marks.</p> <p>The remaining statements are explained separately.</p> |
| <b>Required Privilege Level</b> | <p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Firewall Filter Match Conditions and Actions on page 15</a></li> <li>• <a href="#">Configuring Firewall Filters on page 39</a></li> <li>• <a href="#">Overview of Firewall Filters on page 3</a></li> </ul>                   |

## then (Filters)

---

|                                 |                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>then {<br/>    action;<br/>    action-modifiers;<br/>}</pre>                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit <b>firewall family</b> <i>family-name</i> <b>filter</b> <i>filter-name</i> <b>term</b> <i>term-name</i> ]                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                    |
| <b>Description</b>              | Configure a firewall filter action.                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b>action</b>—Actions to accept, discard, or forward packets that match all conditions specified in a filter term.</p> <p><b>action-modifiers</b>—Additional actions to analyze, classify, count, or police packets that match all conditions specified in a filter term.</p> |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Firewall Filter Match Conditions and Actions on page 15</a></li><li>• <a href="#">Configuring Firewall Filters on page 39</a></li><li>• <a href="#">Understanding Firewall Filter Match Conditions on page 11</a></li></ul>  |



## CHAPTER 10

# Configuration Statements for Policers

- [action](#) on page 196
- [bandwidth-limit](#) on page 196
- [burst-size-limit](#) on page 197
- [color-aware](#) on page 198
- [color-blind](#) on page 199
- [committed-burst-size](#) on page 200
- [committed-information-rate](#) on page 201
- [excess-burst-size](#) on page 202
- [filter-specific](#) on page 203
- [firewall](#) on page 204
- [if-exceeding](#) on page 205
- [loss-priority high then discard \(Three-Color Policer\)](#) on page 206
- [peak-burst-size](#) on page 207
- [peak-information-rate](#) on page 208
- [policer](#) on page 209
- [single-rate](#) on page 210
- [then \(Policers\)](#) on page 211
- [three-color-policer](#) on page 212
- [two-rate](#) on page 213

## action

---

|                                 |                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>action {<br/>    loss-priority high then discard;<br/>}</code>                                                                              |
| <b>Hierarchy Level</b>          | [edit <code>firewall three-color-policer name</code> ]                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.     |
| <b>Description</b>              | Discard traffic on a logical interface using tricolor marking policing.                                                                           |
| <b>Options</b>                  | The statements are explained separately.                                                                                                          |
| <b>Required Privilege Level</b> | <code>firewall</code> —To view this statement in the configuration.<br><code>firewall-control</code> —To add this statement to the configuration. |

## bandwidth-limit

---

|                                 |                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>bandwidth-limit bps;</code>                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit <code>firewall policer policer-name if-exceeding</code> ]                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                             |
| <b>Description</b>              | Specify the traffic rate in bits per second.                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <code>bps</code> —Traffic rate in bits per second. Specify <code>bps</code> as a decimal value or as a decimal number followed by one of the abbreviation <code>k</code> (1000), <code>m</code> (1,000,000), or <code>g</code> (1,000,000,000).<br><b>Range:</b> 32000 bps (32 Kbps) through 10,000,000,000 bps (10 Gbps) |
| <b>Required Privilege Level</b> | <code>firewall</code> —To view this statement in the configuration.<br><code>firewall-control</code> —To add this statement to the configuration.                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li><li>• <a href="#">Overview of Policers on page 61</a></li></ul>                                                                                                            |

---

## burst-size-limit

---

|                                 |                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>burst-size-limit bytes;</code>                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit <code>firewall policer policer-name if-exceeding</code> ]                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                  |
| <b>Description</b>              | Specify the maximum allowed burst size to control the amount of traffic bursting.                                                                                                                              |
| <b>Options</b>                  | <b>bytes</b> —Decimal value or a decimal number followed by k (thousand), m (million), or g (giga).<br><b>Range:</b> 1 through 2,147,450,880 bytes (2147 MB)                                                   |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li><li>• <a href="#">Overview of Policers on page 61</a></li></ul> |

## color-aware

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | color-aware;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit <a href="#">firewall three-color-policer</a> <i>policer-name</i> single-rate],<br>[edit <a href="#">firewall three-color-policer</a> <i>policer-name</i> two-rate]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | Configure the way preclassified packets are metered. In color-aware mode, the switch can assign a higher packet-loss priority, but cannot assign a lower packet loss priority (PLP). For example, suppose an upstream device assigns medium-high PLP to a packet because the packet exceeded its committed information rate (CIR). The switch cannot change the PLP to low even if the packet conforms to the configured CIR of the appropriate interface. On the other hand, if an upstream device assigns low PLP to a packet but the packet exceeds the CIR and committed burst size (CBS) of the switch interface, the switch can increase the PLP to medium-high. |
| <b>Default</b>                  | If you omit the <b>color-aware</b> statement, the default behavior is color-aware mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Overview of Policers on page 61</a></li><li>• <a href="#">Understanding Color-Aware Mode for Single-Rate Tricolor Marking on page 68</a></li><li>• <a href="#">Understanding Color-Aware Mode for Two-Rate Tricolor Marking on page 70</a></li><li>• <a href="#">color-blind on page 199</a></li></ul>                                                                                                                                                                                                                                                                                                             |

## color-blind

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | color-blind;                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit <b>firewall three-color-policer</b> <i>policer-name</i> single-rate],<br>[edit <b>firewall three-color-policer</b> <i>policer-name</i> two-rate]                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | Configure the way preclassified packets are metered. In color-blind mode, the switch ignores any preclassification of packets and can assign a higher or lower packet loss priority (PLP). For example, suppose an upstream device assigns medium-high PLP to a packet because the packet exceeded the CIR on the upstream device. The switch can change the PLP to low if the packet conforms to the CIR of the appropriate interface.                          |
| <b>Default</b>                  | If you omit the <b>color-blind</b> statement, the default behavior is color-aware mode.                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Overview of Policers on page 61</a></li> <li>• <a href="#">Understanding Color-Blind Mode for Single-Rate Tricolor Marking on page 67</a></li> <li>• <a href="#">Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 69</a></li> <li>• <a href="#">Configuring Color-Blind Egress Policers for Medium-Low PLP on page 82</a></li> <li>• <a href="#">color-aware on page 198</a></li> </ul> |

## committed-burst-size

---

|                            |                                                                                                                                                                             |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>committed-burst-size bytes;</code>                                                                                                                                    |
| <b>Hierarchy Level</b>     | [edit <code>firewall three-color-policer policer-name</code> single-rate],<br>[edit <code>firewall three-color-policer policer-name</code> two-rate]                        |
| <b>Release Information</b> | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                               |
| <b>Description</b>         | Configure the maximum number of bytes allowed for incoming traffic to burst above the committed information rate and still be marked with low packet loss priority (green). |




**NOTE:** When you include the `committed-burst-size` statement in the configuration, you must also include the `committed-information-rate` statement at the same hierarchy level.

---


|                                 |                                                                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Options</b>                  | <b>bytes</b> —Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).<br><b>Range:</b> 512 bytes through 268435456 bytes (268 MB) |
| <b>Required Privilege Level</b> | <code>firewall</code> —To view this statement in the configuration.<br><code>firewall-control</code> —To add this statement to the configuration.                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li><li>• <a href="#">Overview of Policers on page 61</a></li></ul>                                                                          |

## committed-information-rate

|                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                      | <code>committed-information-rate <i>bits-per-second</i>;</code>                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                             | [edit <code>firewall three-color-policer <i>policer-name</i> single-rate</code> ],<br>[edit <code>firewall three-color-policer <i>policer-name</i> two-rate</code> ]                                                                                                                                                                        |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                         | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                               |
| <b>Description</b>                                                                                                                                                                                                                                                                                                 | Configure the guaranteed bandwidth under normal line conditions and the average rate up to which packets are marked with low packet loss priority (green).                                                                                                                                                                                  |
| <div>  <p><b>NOTE:</b> When you include the <code>committed-information-rate</code> statement in the configuration, you must also include the <code>committed-burst-size</code> statement at the same hierarchy level.</p> </div> |                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                                                                                                                                                                                                                                                                                                     | <p><b><i>bits-per-second</i></b>—Number of bits per second. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).</p> <p><b>Range:</b> 32,000 bps through 10,000,000,000 bps (10 gbps)</p> |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                    | <p><code>firewall</code>—To view this statement in the configuration.</p> <p><code>firewall-control</code>—To add this statement to the configuration.</p>                                                                                                                                                                                  |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                       | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li> <li>• <a href="#">Overview of Policers on page 61</a></li> </ul>                                                                                                                           |

## excess-burst-size

---

|                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                 | <code>excess-burst-size bytes;</code>                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                        | [edit <code>firewall three-color-policer policer-name</code> single-rate]                                                                                                                                                                                                               |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                    | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                           |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                            | Configure the maximum number of bytes allowed for incoming traffic to burst above the committed information rate and still be marked with medium-high packet loss priority (yellow). Packets that exceed the excess burst size (EBS) are marked with high packet loss priority (red).   |
| <div> <b>NOTE:</b> When you include the <code>excess-burst-size</code> statement in the configuration, you must also include the <code>committed-burst-size</code> and <code>committed-information-rate</code> statements at the same hierarchy level.</div> |                                                                                                                                                                                                                                                                                         |
| <b>Options</b>                                                                                                                                                                                                                                                                                                                                | <b>bytes</b> —Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).<br><b>Range:</b> 512 bytes through 268435456 bytes (268 MB) |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                               | <code>firewall</code> —To view this statement in the configuration.<br><code>firewall-control</code> —To add this statement to the configuration.                                                                                                                                       |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"><li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li><li>• <a href="#">Overview of Policers on page 61</a></li></ul>                                                                          |



---

## filter-specific

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | filter-specific;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit <b>firewall policer</b> <i>policer-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>              | <p>Configure a policer to be filter-specific, which means that Junos OS creates only one policer instance regardless of how many times the policer is referenced. If you use a filter-specific policer in multiple terms, both of the following are true:</p> <ul style="list-style-type: none"><li>• Traffic is policed at the aggregate rate. For example, if you create a policer that has a bandwidth limit of 100 Mbps and use the policer in two terms, the total allowed bandwidth for both terms is 100 Mbps—not 100 Mbps for each term.</li><li>• The implicit counter counts all the packets are that matched by any of the terms. For example, if you reference the same filter-specific policer in term1 and term2, and term1 matches 1000 packets and term2 matches 500 packets, the implicit counter shows 1500 matches for the policer.</li></ul> |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li><li>• <a href="#">Overview of Policers on page 61</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## firewall

```

Syntax firewall {
 family family-name {
 filter filter-name {
 interface-specific;
 term term-name {
 from {
 match-conditions;
 }
 then {
 action;
 action-modifiers;
 }
 }
 }
 }
 policer policer-name {
 filter-specific;
 if-exceeding {
 bandwidth-limit bps;
 burst-size-limit bytes;
 }
 then {
 policer-action;
 }
 }
 three-color-policer policer-name {
 action {
 loss-priority high then discard;
 }
 single-rate {
 (color-aware | color-blind);
 committed-information-rate bps;
 committed-burst-size bytes;
 excess-burst-size bytes;
 }
 two-rate {
 (color-aware | color-blind);
 committed-information-rate bps;
 committed-burst-size bytes;
 peak-information-rate bps;
 peak-burst-size bytes;
 }
 }
 }

```

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 firewall filters and policers.

The remaining statements are explained separately.

|                                 |                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Firewall Filter Match Conditions and Actions on page 15</a></li> <li>• <a href="#">Configuring Firewall Filters on page 39</a></li> <li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li> <li>• <a href="#">Overview of Firewall Filters on page 3</a></li> </ul> |

## if-exceeding


|                                 |                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>if-exceeding {     bandwidth-limit <i>bps</i>;     burst-size-limit <i>bytes</i>; }</pre>                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit <a href="#">firewall policer</a> <i>policer-name</i> ]                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                     |
| <b>Description</b>              | <p>Configure policer rate limits.</p> <p>The remaining statements are explained separately.</p>                                                                                                                   |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li> <li>• <a href="#">Overview of Policers on page 61</a></li> </ul> |

## loss-priority high then discard (Three-Color Policer)

---


|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | loss-priority high then discard;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit firewall <b>three-color-policer</b> <i>policer-name</i> <b>action</b> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | <p>For packets with high loss priority, discard the packets. The loss priority setting is not configurable. Include this statement if you do not want the switch to forward packets that have high packet-loss priority.</p> <p>For single-rate three-color policers, Junos OS assigns high loss priority to packets that exceed the committed information rate and the excess burst size.</p> <p>For two-rate three-color policers, Junos OS assigns high loss priority to packets that exceed the peak information rate and the peak burst size.</p> |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li><li>• <a href="#">Overview of Policers on page 61</a></li></ul>                                                                                                                                                                                                                                                                                                                                         |

## peak-burst-size

|                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                   | <code>peak-burst-size bytes;</code>                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                          | [edit <code>firewall three-color-policer policer-name two-rate</code> ]                                                                                                                                                                                                                                  |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                            |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                              | Configure the maximum number of bytes allowed for incoming packets to burst above the peak information rate (PIR) and still be marked with medium-high packet loss priority (yellow). Packets that exceed the peak burst size (PBS) are marked with high packet loss priority (red).                     |
| <div>  <p><b>NOTE:</b> When you include the <code>peak-burst-size</code> statement in the configuration, you must also include the <code>committed-burst-size</code> and <code>peak-information-rate</code> statements at the same hierarchy level.</p> </div> |                                                                                                                                                                                                                                                                                                          |
| <b>Options</b>                                                                                                                                                                                                                                                                                                                                  | <p><b>bytes</b>—Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).</p> <p><b>Range:</b> 1500 bytes through 100,000,000,000 bytes (100 GB)</p> |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                                 | <p><code>firewall</code>—To view this statement in the configuration.</p> <p><code>firewall-control</code>—To add this statement to the configuration.</p>                                                                                                                                               |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li> <li>• <a href="#">Overview of Policers on page 61</a></li> </ul>                                                                                        |

## peak-information-rate

---

|                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                | <code>peak-information-rate <i>bits-per-second</i>;</code>                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                       | [ <a href="#">edit</a> <code>firewall three-color-policer <i>policer-name</i> two-rate</code> ]                                                                                                                                                                                                                                                           |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                   | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                             |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                           | Configure the maximum achievable rate. Packets that exceed the committed information rate (CIR) but are below the peak information rate (PIR) are marked with medium-high packet loss priority (yellow). Packets that exceed the PIR are marked with high packet loss priority (red). You can configure a discard action for packets that exceed the PIR. |
| <div> <b>NOTE:</b> When you include the <code>peak-information-rate</code> statement in the configuration, you must also include the <code>committed-information-rate</code> and <code>peak-burst-size</code> statements at the same hierarchy level.</div> |                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>                                                                                                                                                                                                                                                                                                                               | <b><i>bits-per-second</i></b> —Number of bits per second. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).<br><b>Range:</b> 32,000 bps through 10,000,000,000 bps (10 gbps)                         |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                              | <code>firewall</code> —To view this statement in the configuration.<br><code>firewall-control</code> —To add this statement to the configuration.                                                                                                                                                                                                         |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"><li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li><li>• <a href="#">Overview of Policers on page 61</a></li></ul>                                                                                                                                            |

## policer

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> policer <i>policer-name</i> {     filter-specific;     if-exceeding {         bandwidth-limit <i>bps</i>;         burst-size-limit <i>bytes</i>;     }     then {         <i>policer-action</i>;     } } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit <a href="#">firewall</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | <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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | <p>Configure policer rate limits and actions. To activate a policer, you must include the <b>policer</b> action modifier in the <b>then</b> statement in a firewall filter term.</p> <p>Each policer that you configure includes an implicit counter that counts the number of packets that exceed the rate limits that are specified for the policer. If you use the same policer in multiple terms—either within the same filter or across filters—the policer’s implicit counter is used to count packets that are policed in all of these terms. If you want to obtain separate packet counts for each term, use these approaches:</p> <ul style="list-style-type: none"> <li>• Configure a unique policer for each term.</li> <li>• Configure only one policer, but use a unique, explicit counter in each term.</li> </ul> |
| <b>Options</b>                  | <p><b><i>policer-name</i></b>—Name that identifies the policer. The name can contain letters, numbers, hyphens (-), and can be up to 64 characters long.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Required Privilege Level</b> | <p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li> <li>• <a href="#">Configuring Firewall Filters on page 39</a></li> <li>• <a href="#">Overview of Policers on page 61</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |


## single-rate

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>single-rate {<br/>  (color-aware   color-blind);<br/>  committed-information-rate <i>bps</i>;<br/>  committed-burst-size <i>bytes</i>;<br/>  excess-burst-size <i>bytes</i>;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit <a href="#">firewall three-color-policer</a> <i>policer-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | <p>Configure a single-rate three-color policer in which marking is based on the committed information rate (CIR), committed burst size (CBS), and excess burst size (EBS).</p> <p>Packets that conform to the CIR or the CBS are assigned low loss priority (green). Packets that exceed the CIR and the CBS but are within the EBS are assigned medium-high loss priority (yellow). Packets that exceed the EBS are assigned high loss priority (red).</p> <p>Green and yellow packets are always forwarded; this action is not configurable. You can configure red packets to be discarded. By default, red packets are forwarded.</p> <p>The remaining statements are explained separately.</p> |
| <b>Options</b>                  | <b><i>policer-name</i></b> —Name of the three-color policer. Use this name when you apply the policer to an interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Required Privilege Level</b> | <b>firewall</b> —To view this statement in the configuration.<br><b>firewall-control</b> —To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li><li>• <a href="#">Overview of Policers on page 61</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



## then (Policers)

|                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                           | then {<br><i>policer-action</i> ;<br>}                                                                                                                                                                                                                                                                                            |
| <b>Hierarchy Level</b>                                                                                                                                                                                                  | [edit <b>firewall</b> <b>policer</b> <i>policer-name</i> ]                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>                                                                                                                                                                                              | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                     |
| <b>Description</b>                                                                                                                                                                                                      | Configure a policer action.                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                                                                                                                                                                                                          | <i>policer-action</i> —Allowed policer actions are <b>discard</b> , <b>loss-priority high</b> , and <b>loss-priority low</b> . <b>discard</b> causes the system to drop traffic that exceeds the rate limits defined by the policer. Use <b>loss-priority high</b> to allow the system to forward matching traffic in some cases. |
| <div>  <b>NOTE:</b> If you specify a policer in an egress firewall filter, the only supported action is <b>discard</b>.         </div> |                                                                                                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b>                                                                                                                                                                                         | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                             |
| <b>Related Documentation</b>                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li> <li>• <a href="#">Configuring Firewall Filters on page 39</a></li> <li>• <a href="#">Overview of Policers on page 61</a></li> </ul>                                              |

## three-color-policer

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> three-color-policer <i>policer-name</i> {   action {     loss-priority high then discard;   }   single-rate {     (color-aware   color-blind);     committed-information-rate <i>bps</i>;     committed-burst-size <i>bytes</i>;     excess-burst-size <i>bytes</i>;   }   two-rate {     (color-aware   color-blind);     committed-information-rate <i>bps</i>;     committed-burst-size <i>bytes</i>;     peak-information-rate <i>bps</i>;     peak-burst-size <i>bytes</i>;   } } </pre> |
| <b>Hierarchy Level</b>          | [edit <a href="#">firewall</a> ],<br>[edit logical-systems <i>logical-system-name</i> firewall]                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Configure a three-color policer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Options</b>                  | <p><b><i>policer-name</i></b>—Name of the three-color policer. Use this name when you apply the policer to an interface.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                              |
| <b>Required Privilege Level</b> | firewall—To view this statement in the configuration.<br>firewall-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 82</a></li> <li><a href="#">Overview of Policers on page 61</a></li> </ul>                                                                                                                                                                                                                                                                                       |

## two-rate

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>two-rate {   (color-aware   color-blind);   committed-information-rate <i>bps</i>;   committed-burst-size <i>bytes</i>;   peak-information-rate <i>bps</i>;   peak-burst-size <i>bytes</i>; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit <b>firewall three-color-policer</b> <i>policer-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | <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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | <p>Configure a two-rate three-color policer in which marking is based on the committed information rate (CIR), committed burst size (CBS), peak information rate (PIR), and peak burst size (PBS).</p> <p>Packets that conform to the CIR or the CBS are assigned low loss priority (green). Packets that exceed the CIR and the CBS but are within the PIR or the PBS are assigned medium-high loss priority (yellow). Packets that exceed the PIR and the PBS are assigned high loss priority (red).</p> <p>Green and yellow packets are always forwarded; this action is not configurable. You can configure red packets to be discarded. By default, red packets are forwarded.</p> <p>The remaining statements are explained separately.</p> |
| <b>Required Privilege Level</b> | <p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |



## CHAPTER 11

# Configuration Statements for MACsec

- cak on page 216
- ckn on page 217
- connectivity-association on page 218
- connectivity-association (MACsec Interfaces) on page 219
- direction on page 220
- encryption on page 221
- exclude-protocol on page 222
- id on page 223
- include-sci on page 224
- interfaces (MACsec) on page 225
- key on page 226
- key-server-priority on page 227
- mac-address (MACsec) on page 228
- macsec on page 229
- mka on page 230
- must-secure on page 231
- no-encryption on page 232
- offset on page 233
- port-id on page 234
- pre-shared-key on page 235
- replay-protect on page 236
- replay-window-size on page 237
- secure-channel on page 238
- security-association on page 239
- security-mode on page 240
- transmit-interval (MACsec) on page 241

## cak

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <i>ckn hexadecimal-number;</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit security <a href="#">macsec connectivity-association</a> <i>connectivity-association-name</i> <a href="#">pre-shared-key</a> ]                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | <p>Specifies the connectivity association key (CAK) for a pre-shared key.</p> <p>A pre-shared key includes a connectivity association key name (CKN) and a CAK. A pre-shared key is exchanged between two devices at each end of a point-to-point link to enable MACsec using dynamic security keys. The MACsec Key Agreement (MKA) protocol is enabled once the pre-shared keys are successfully exchanged. The pre-shared key—the CKN and CAK—must match on both ends of a link</p> |
| <b>Default</b>                  | No CAK exists, by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <p><i>hexadecimal-number</i>—The key name, in hexadecimal format.</p> <p>The key name is 32 hexadecimal characters in length. If you enter a key name that is less than 32 characters long, the remaining characters are set to 0.</p>                                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li></ul>                                                                                                                                                                                                                                                                                                                                                       |

## ckn

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>ckn <i>hexadecimal-number</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit security <a href="#">macsec connectivity-association</a> <i>connectivity-association-name</i> <a href="#">pre-shared-key</a> ]                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | <p>Specifies the connectivity association key name (CKN) for a pre-shared key.</p> <p>A pre-shared key includes a CKN and a connectivity association key (CAK). A pre-shared key is exchanged between two devices at each end of a point-to-point link to enable MACsec using dynamic security keys. The MACsec Key Agreement (MKA) protocol is enabled once the pre-shared keys are successfully exchanged. The pre-shared key—the CKN and CAK—must match on both ends of a link</p> |
| <b>Default</b>                  | No CKN exists, by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <p><i>hexadecimal-number</i>—The key name, in hexadecimal format.</p> <p>The key name is 32 hexadecimal characters in length. If you enter a key name that is less than 32 characters long, the remaining characters are set to 0.</p>                                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                       |

## connectivity-association

**Syntax** `connectivity-association connectivity-association-name {  
     exclude-protocol protocol-name;  
     include-sci;  
     mka {  
         must-secure;  
         key-server-priority priority-number;  
         transmit-interval interval;  
     }  
     no-encryption;  
     offset (0|30|50);  
     pre-shared-key {  
         cak hexadecimal-number;  
         ckn hexadecimal-number;  
     }  
     replay-protect {  
         replay-window-size number-of-packets;  
     }  
     secure-channel secure-channel-name {  
         direction (inbound | outbound);  
         encryption;  
         id {  
             mac-address mac-address;  
             port-id port-id-number;  
         }  
         offset (0|30|50);  
         security-association security-association-number {  
             key key-string;  
         }  
     }  
     security-mode security-mode;  
 }`

**Hierarchy Level** [edit security *macsec*]

**Release Information** Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.  
 Statement introduced in Junos OS Release 14.1X53-D15 for the QFX Series.

**Description** Create or configure a MACsec connectivity association.

A connectivity association is not applying MACsec to traffic until it is associated with an interface. MACsec connectivity associations are associated with interfaces using the *interfaces* statement in the [edit security macsec] hierarchy.

**Default** No connectivity associations are present, by default.

**Options** The remaining statements are explained separately.

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



**Related Documentation** • [Configuring Media Access Control Security \(MACsec\) on page 99](#)

## connectivity-association (MACsec Interfaces)

---

|                                 |                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>connectivity-association <i>connectivity-association-name</i>;</code>                                                                                   |
| <b>Hierarchy Level</b>          | [edit security <a href="#">macsec interfaces</a> <i>interface-name</i> ]                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches. |
| <b>Description</b>              | Applies a connectivity association to an interface, which enables Media Access Control Security (MACsec) on that interface.                                   |
| <b>Default</b>                  | No connectivity associations are associated with any interfaces.                                                                                              |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                               |
| <b>Related Documentation</b>    | • <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a>                                                                               |

## direction

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>direction (inbound   outbound);</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit security <code>macsec connectivity-association connectivity-association-name secure-channel secure-channel-name</code> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | <p>Configure whether the secure channel applies MACsec security to traffic entering or leaving an interface.</p> <p>If you need to apply MACsec on traffic entering and leaving an interface, you need to create one secure channel to apply MACsec on incoming traffic and another secure channel to apply MACsec on outgoing traffic within the same connectivity association. When you associate the connectivity association with an interface, MACsec is applied on traffic entering and leaving that interface.</p> <p>You only use this configuration option when you are configuring MACsec using static secure association keys (SAK) security mode. When you are configuring MACsec using static connectivity association keys (CAK) security mode, two secure channels that are not user-configurable—one inbound secure channel and one outbound secure channel—are automatically created within the connectivity association.</p> |
| <b>Default</b>                  | <p>This statement does not have a default value.</p> <p>If you have configured a secure channel to enable MACsec using static SAK security mode, you must specify whether the secure channel applies MACsec to traffic entering or leaving an interface. A candidate configuration that contains a secure channel that has not configured a direction cannot be committed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Options</b>                  | <p><b>inbound</b>—Enable MACsec security on traffic entering the interface that has applied the secure channel.</p> <p><b>outbound</b>—Enable MACsec security on traffic leaving the interface that has applied the secure channel.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## encryption

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | encryption;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit security <b>macsec</b> <b>connectivity-association</b> <i>connectivity-association-name</i> <b>secure-channel</b> <i>secure-channel-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | <p>Enable MACsec encryption within a secure channel.</p> <p>You can enable MACsec without enabling encryption. If a connectivity association with a secure channel that has not enabled MACsec encryption is associated with an interface, traffic is forwarded across the Ethernet link in clear text. You are, therefore, able to view this unencrypted traffic when you are monitoring the link. The MACsec header is still applied to the frame, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic has not been tampered with and does not represent a security threat.</p> <p>Traffic traversing a MAC-enabled point-to-point Ethernet link traverses the link at the same speed regardless of whether encryption is enabled or disabled. You cannot increase the speed of traffic traversing a MACsec-enabled Ethernet link by disabling encryption.</p> <p>This command is used to enable encryption when MACsec is configured using secure association key (SAK) security mode only. When MACsec is configuring using static connectivity association key (CAK) security mode, the encryption setting is configured outside of the secure channel using the <b>no-encryption</b> configuration statement.</p> |
| <b>Default</b>                  | MACsec encryption is disabled when MACsec is configured using static SAK security mode, by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## exclude-protocol

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>exclude-protocol <i>protocol-name</i>;</code>                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | [edit security <a href="#">macsec connectivity-association</a> <i>connectivity-association-name</i> ]                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                     |
| <b>Description</b>              | <p>Specifies protocols whose packets are not secured using Media Access Control Security (MACsec) when MACsec is enabled on a link using static connectivity association key (CAK) security mode.</p> <p>When this option is enabled in a connectivity association that is attached to an interface, MACsec is not enabled for all packets of the specified protocols that are sent and received on the link.</p> |
| <b>Default</b>                  | <p>Disabled.</p> <p>All packets are secured on a link when MACsec is enabled, with the exception of all types of Spanning Tree Protocol (STP) packets.</p>                                                                                                                                                                                                                                                        |
| <b>Options</b>                  | <p><b><i>protocol-name</i></b>—Specifies the name of the protocol that should not be MACsec-secured. Options include:</p> <ul style="list-style-type: none"><li>• <b>cdp</b>—Cisco Discovery Protocol.</li><li>• <b>lcp</b>—Link Aggregation Control Protocol.</li><li>• <b>lldp</b>—Link Level Discovery Protocol.</li></ul>                                                                                     |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li></ul>                                                                                                                                                                                                                                                                                   |

## id

---

|                                 |                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | id {<br><code>mac-address</code> <i>mac-address</i> ;<br><code>port-id</code> <i>port-id-number</i> ;<br>}                                                                             |
| <b>Hierarchy Level</b>          | [edit security <code>macsec connectivity-association</code> <i>connectivity-association-name</i> <code>secure-channel</code> <i>secure-channel-name</i> ]                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                          |
| <b>Description</b>              | Specify a MAC address and a port that traffic on the link must be from to be accepted by the interface when MACsec is enabled using static secure association key (SAK) security mode. |
| <b>Options</b>                  | The remaining statements are explained separately.                                                                                                                                     |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li> </ul>                                                      |

## include-sci

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | include-sci;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit security <b>macsec connectivity-association</b> <i>connectivity-association-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | <p>Specifies that the SCI tag should be appended to each packet on a link that has enabled MACsec.</p> <p>You must enable SCI tagging on a switch that is enabling MACsec on an Ethernet link connecting to an EX4300 switch.</p> <p>SCI tags are automatically appended to packets leaving a MACsec-enabled interface on an EX4300 switch. This option is, therefore, not available on EX4300 switches.</p> <p>You should only use this option when connecting a switch to an EX4300 switch, or to a host device that requires SCI tagging. SCI tags are eight octets long, so appending an SCI tag to all traffic on the link adds a significant amount of unneeded overhead.</p> |
| <b>Default</b>                  | <p>SCI tagging is enabled on EX4300 switches that have enabled MACsec using static connectivity association key (CAK) security mode, by default.</p> <p>SCI tagging is disabled on all other interfaces, by default.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## interfaces (MACsec)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> interfaces <i>interface-name</i> {     <a href="#">connectivity-association</a> <i>connectivity-association-name</i>; } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit security <a href="#">macsec</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | <p>Applies the specified connectivity association to the specified interface to enable MACsec.</p> <p>One connectivity association can be applied to multiple interfaces.</p> <p>You must always use this statement to apply a connectivity association to an interface to enable MACsec. You must complete this configuration step regardless of whether MACsec is enabled using static connectivity association key (CAK) security mode or static secure association key (SAK) security mode.</p> <p>If you are enabling MACsec using static SAK security mode and need to configure MACsec on inbound and outbound traffic on the same interface, you must configure a connectivity association with one secure channel for inbound traffic and a second secure channel for outbound traffic. The connectivity association is then applied to the interface using this statement to enable MACsec for traffic entering and leaving the interface.</p> |
| <b>Default</b>                  | Interfaces are not associated with any connectivity associations, by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## key

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>key key-string;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit security <a href="#">macsec connectivity-association connectivity-association-name secure-channel secure-channel-name security-association security-association-number</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | <p>Specifies the static security key to exchange to enable MACsec using static secure association key (SAK) security mode.</p> <p>The key string is a 32-digit hexadecimal number. The key string and the security association must match on both sides of an Ethernet connection to secure traffic using MACsec when enabling MACsec using SAK security mode.</p> <p>You must configure at least two security associations with unique security association numbers and key strings to enable MACsec using static SAK security mode. MACsec initially establishes a secure connection when a security association number and key match on both ends of an Ethernet link. After a certain number of Ethernet frames are securely transmitted across the Ethernet link, MACsec automatically rotates to a new security association with a new security association number and key to maintain the secured Ethernet link. This rotation continues each time a certain number of Ethernet frames are securely transmitted across the secured Ethernet link, so you must always configure MACsec to have at least two security associations.</p> |
| <b>Default</b>                  | This statement does not have a default value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Options</b>                  | <b>key-string</b> —Specifies the key to exchange with the other end of the link on the secure channel. The <i>key-string</i> is a 32-digit hexadecimal string that is created by the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



## key-server-priority

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>key-server-priority <i>priority-number</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit security <b>macsec</b> <b>connectivity-association</b> <i>connectivity-association-name</i> mka]                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | <p>Specifies the key server priority used by the MACsec Key Agreement (MKA) protocol to select the key server when MACsec is enabled using static connectivity association key (CAK) security mode.</p> <p>The switch with the lower <i>priority-number</i> is selected as the key server.</p> <p>If the <i>priority-number</i> is identical on both sides of a point-to-point link, the MKA protocol selects the device with the lower MAC address as the key server.</p> |
| <b>Default</b>                  | The default key server priority number is 16.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Options</b>                  | <p><b><i>priority-number</i></b>—Specifies the MKA server election priority number.</p> <p>The <i>priority-number</i> can be any number between 0 and 255. The lower the number, the higher the priority.</p>                                                                                                                                                                                                                                                              |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li> </ul>                                                                                                                                                                                                                                                                                                                                          |

## mac-address (MACsec)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>mac-address <i>mac-address</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit security <a href="#">macsec connectivity-association</a> <i>connectivity-association-name</i> <a href="#">secure-channel</a> <i>secure-channel-name id</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | <p>Specify a MAC address to enable MACsec using static secure association key (SAK) security mode. The <b>mac-address</b> variables must match on the sending and receiving ends of a link to enable MACsec using static SAK security mode.</p> <p>If you are configuring a MAC address on a secure channel in the outbound direction, you should specify the MAC address of the interface as the <b>mac-address</b>.</p> <p>If you are configuring a MAC address on a secure channel in the inbound direction, you should specify the MAC address of the interface at the other end of the link as the <b>mac-address</b>.</p> <p>You only use this configuration option when you are configuring MACsec using static SAK security mode. This option does not need to be specified when you are enabling MACsec using static connectivity association key (CAK) security mode.</p> |
| <b>Default</b>                  | No MAC address is specified in the secure channel, by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Options</b>                  | <b>mac-address</b> —The MAC address, in six groups of two hexadecimal digits.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## macsec

```
Syntax macsec {
 connectivity-association connectivity-association-name {
 exclude-protocol protocol-name;
 include-sci;
 mka {
 must-secure;
 key-server-priority priority-number;
 transmit-interval interval;
 }
 no-encryption;
 offset (0|30|50);
 pre-shared-key {
 cak hexadecimal-number;
 ckn hexadecimal-number;
 }
 replay-protect {
 replay-window-size number-of-packets;
 }
 secure-channel secure-channel-name {
 direction (inbound | outbound);
 encryption;
 id {
 mac-address mac-address;
 port-id port-id-number;
 }
 offset (0|30|50);
 security-association security-association-number {
 key key-string;
 }
 }
 security-mode security-mode;
 }
 interfaces interface-name {
 connectivity-association connectivity-association-name;
 }
 }
```

**Hierarchy Level** [edit security]

**Release Information** Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.  
Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.

**Description** Configure Media Access Control Security (MACsec)..

**Options** The remaining statements are explained separately.

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

**Related Documentation**

- [Configuring Media Access Control Security \(MACsec\) on page 99](#)

## mka

---

|                                 |                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>mka {<br/>    must-secure;<br/>    key-server-priority <i>priority-number</i>;<br/>    transmit-interval <i>interval</i>;<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit security <a href="#">macsec connectivity-association</a> <i>connectivity-association-name</i> ]                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15.<br>Statement introduced in Junos OS Release 14.1X53-D15 for the QFX Series.          |
| <b>Description</b>              | Specify parameters for the MACsec Key Agreement (MKA) protocol.                                                                            |
| <b>Options</b>                  | The remaining statements are explained separately.                                                                                         |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li></ul>            |

## must-secure

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>must-secure;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | <code>[edit security <b>macsec</b> <b>connectivity-association</b> <i>connectivity-association-name</i> <b>mka</b>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.1X53-D10.<br>Statement introduced in Junos OS Release 14.1X53-D15 for the QFX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | <p>Specifies that all traffic travelling on the MACsec-secured link must be MACsec-secured to be forwarded onward.</p> <p>When the <b>must-secure</b> option is enabled, all traffic that is not MACsec-secured that is received on the interface is dropped.</p> <p>When the <b>must-secure</b> option is disabled, all traffic from devices that support MACsec is MACsec-secured while traffic received from devices that do not support MACsec is forwarded through the network.</p> <p>The <b>must-secure</b> option is particularly useful in scenarios where multiple devices, such as a phone and a PC, are accessing the network through the same Ethernet interface. If one of the devices supports MACsec while the other device does not support MACsec, the device that doesn't support MACsec can continue to send and receive traffic over the network—provided the <b>must-secure</b> option is disabled—while traffic to and from the device that supports MACsec is MACsec-secured. In this scenario, traffic to the device that is not MACsec-secured must be VLAN-tagged.</p> |
| <b>Default</b>                  | The <b>must-secure</b> option is disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## no-encryption

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | no-encryption;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit security <b>macsec connectivity-association</b> <i>connectivity-association-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | <p>Disables MACsec encryption for a connectivity association that is configured to enable MACsec using static connectivity association key (CAK) or dynamic security mode.</p> <p>You can enable MACsec without enabling encryption. If a connectivity association that has not enabled MACsec encryption is associated with an interface, traffic is forwarded across the Ethernet link in clear text. You are, therefore, able to view this unencrypted traffic when you are monitoring the link. The MACsec header is still applied to the packet, however, and all MACsec data integrity checks are run on both ends of the link to ensure the traffic does not represent a security threat.</p> <p>This command is used to disable encryption when MACsec is configured using static CAK or dynamic security mode only. When MACsec is configuring using static secure association key (SAK) security mode, the encryption setting is managed in the secure channel using the <b>encryption</b> configuration statement.</p> |
| <b>Default</b>                  | MACsec encryption is enabled if MACsec is enabled using static CAK or dynamic security mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## offset

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | offset (0  30   50);                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>     | [edit security <b>macsec connectivity-association</b> <i>connectivity-association-name</i> ]<br>[edit security <b>macsec connectivity-association</b> <i>connectivity-association-name</i> <b>secure-channel</b> <i>secure-channel-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b> | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>         | <p>Specifies the number of octets in an Ethernet frame that are sent in unencrypted plain-text when encryption is enabled for MACsec.</p> <p>Setting the offset to 30 allows a feature to see the IPv4 header and the TCP/UDP header while encrypting the remaining traffic. Setting the offset to 50 allows a feature to see the IPv6 header and the TCP/UDP header while encrypting the remaining traffic.</p> <p>You would typically forward traffic with the first 30 or 50 octets unencrypted if a feature needed to see the data in the octets to perform a function, but you otherwise prefer to encrypt the remaining data in the frames traversing the link. Load balancing features, in particular, typically need to see the IP and TCP/UDP headers in the first 30 or 50 octets to properly load balance traffic.</p> <p>You configure the <b>offset</b> in the [edit security <b>macsec connectivity-association</b> <i>connectivity-association-name</i>] hierarchy when you are enabling MACsec using static connectivity association key (CAK) or dynamic security mode.</p> <p>You configure the <b>offset</b> in the [edit security <b>macsec connectivity-association</b> <i>connectivity-association-name</i> <b>secure-channel</b> <i>secure-channel-name</i>] hierarchy when you are enabling MACsec using static secure association key (SAK) security mode.</p> |
| <b>Default</b>             | 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>             | <p><b>0</b>—Specifies that no octets are unencrypted. When you set the offset to 0, all traffic on the interface where the connectivity association or secure channel is applied is encrypted.</p> <p><b>30</b>—Specifies that the first 30 octets of each Ethernet frame are unencrypted.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



**NOTE:** In IPv4 traffic, setting the offset to 30 allows a feature to see the IPv4 header and the TCP/UDP header while encrypting the rest of the traffic. An offset of 30, therefore, is typically used when a feature needs this information to perform a task on IPv4 traffic.

**50**—Specified that the first 50 octets of each Ethernet frame are unencrypted.



**NOTE:** In IPv6 traffic, setting the offset to 50 allows a feature to see the IPv6 header and the TCP/UDP header while encrypting the rest of the traffic. An offset of 50, therefore, is typically used when a feature needs this information to perform a task on IPv6 traffic.

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

**Related Documentation**

- [Configuring Media Access Control Security \(MACsec\) on page 99](#)

## port-id

**Syntax** `port-id port-id-number;`

**Hierarchy Level** [edit security [macsec connectivity-association](#) *connectivity-association-name* [secure-channel](#) *secure-channel-name* **id**]

**Release Information** Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.  
Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.

**Description** Specify a port ID in a secure channel when enabling MACsec using static secure association key (SAK) security mode. The port IDs must match on a sending and receiving secure channel on each side of a link to enable MACsec.

Once the port numbers match, MACsec is enabled for all traffic on the connection.

You only use this configuration option when you are configuring MACsec using static SAK security mode. This option does not need to be specified when you are enabling MACsec using static connectivity association key (CAK) security mode.

**Default** No port ID is specified.

**Options** *port-id-number*—The port ID number.

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

**Related Documentation**

- [Configuring Media Access Control Security \(MACsec\) on page 99](#)



## pre-shared-key

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>pre-shared-key {     cak hexadecimal-number;     ckn hexadecimal-number; }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>          | [edit security <b>macsec</b> <b>connectivity-association</b> <i>connectivity-association-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Description</b>              | <p>Specifies the pre-shared key used to enable MACsec using static connectivity association key (CAK) security mode.</p> <p>A pre-shared key includes a connectivity association key name (CKN) and a connectivity association key (CAK). A pre-shared key is exchanged between two devices at each end of a point-to-point link to enable MACsec using static CAK security mode. The MACsec Key Agreement (MKA) protocol is enabled after the pre-shared keys are successfully verified and exchanged. The pre-shared key—the CKN and CAK—must match on both ends of a link.</p> |
| <b>Default</b>                  | No pre-shared keys exist, by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Options</b>                  | The remaining statements are explained separately.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## replay-protect

---

|                                 |                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>replay-protect {<br/>    <a href="#">replay-window-size</a> <i>number-of-packets</i>;<br/>}</pre>                                                                                                           |
| <b>Hierarchy Level</b>          | [edit security <a href="#">macsec</a> <a href="#">connectivity-association</a> <i>connectivity-association-name</i> ]                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                    |
| <b>Description</b>              | <p>Enable replay protection for MACsec.</p> <p>A replay window size specified using the <a href="#">replay-window-size</a> <i>number-of-packets</i> statement must be specified to enable replay protection.</p> |
| <b>Options</b>                  | The remaining statements are explained separately.                                                                                                                                                               |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li></ul>                                                                                  |

## replay-window-size

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>replay-window-size <i>number-of-packets</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit security <a href="#">macsec connectivity-association</a> <i>connectivity-association-name</i> replay-protect]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | <p>Specifies the size of the replay protection window.</p> <p>This statement has to be configured to enable replay protection.</p> <p>When MACsec is enabled on an Ethernet link, an ID number is assigned to each packet entering the link. The ID number of the packet is checked by the receiving interface after the packet has traversed the MACsec-enabled link.</p> <p>When replay protection is enabled, the sequence of the ID number of received packets are checked. If the packet arrives out of sequence and the difference between the packet numbers exceeds the replay protection window size, the packet is dropped by the receiving interface. For instance, if the replay protection window size is set to five and a packet assigned the ID of 1006 arrives on the receiving link immediately after the packet assigned the ID of 1000, the packet that is assigned the ID of 1006 is dropped because it falls outside the parameters of the replay protection window.</p> <p>Replay protection is especially useful for fighting man-in-the-middle attacks. A packet that is replayed by a man-in-the-middle attacker on the Ethernet link will arrive on the receiving link out of sequence, so replay protection helps ensure the replayed packet is dropped instead of forwarded through the network.</p> <p>Replay protection should not be enabled in cases where packets are expected to arrive out of order.</p> |
| <b>Default</b>                  | Replay protection is disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                  | <p><i>number-of-packets</i>—Specifies the size of the replay protection window, in packets.</p> <p>When this variable is set to 0, all packets that arrive out-of-order are dropped.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## secure-channel

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>secure-channel <i>secure-channel-name</i> {<br/>    <b>direction</b> (inbound   outbound);<br/>    <b>encryption</b>;<br/>    <b>id</b> {<br/>        <b>mac-address</b> <i>mac-address</i>;<br/>        <b>port-id</b> <i>port-id-number</i>;<br/>    }<br/>    <b>offset</b> (0 30 50);<br/>    <b>security-association</b> <i>security-association-number</i> {<br/>        <b>key</b> <i>key-string</i>;<br/>    }<br/>}</pre>                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit security <b>macsec</b> <b>connectivity-association</b> <i>connectivity-association-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | <p>Create and configure a secure channel to enable and configure MACsec when MACsec is enabled using static secure association key (SAK) security mode.</p> <p>You do not need to use this option to enable MACsec using static connectivity association key (CAK) security mode. All configuration for MACsec using static CAK security mode is done inside of the connectivity association but outside of the secure channel. When MACsec is enabled using static CAK security mode, an inbound and an outbound secure channel—neither of which is user-configurable—is automatically created within the connectivity association.</p> |
| <b>Options</b>                  | The remaining statements are explained separately.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | <b>admin</b> —To view this statement in the configuration.<br><b>admin-control</b> —To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## security-association

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>security-association <i>security-association-number</i> {<br/>    key <i>key-string</i>;<br/>}</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | <code>[edit security <i>macsec</i> connectivity-association <i>connectivity-association-name</i> secure-channel<br/>    <i>secure-channel-name</i>]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | <p>Specifies the number of one of the security associations in the secure channel when MACsec is enabled using static secure association key (SAK) security mode. Because SAKs are created by the key server when MACsec is enabled using static connectivity association key (CAK) security mode, the <b>security-association</b> statement is not used when enabling MACsec using static CAK security mode.</p> <p>You must configure at least two security associations to enable MACsec using static SAK security mode. MACsec initially establishes a secure connection when a security association number and key match on both ends of an Ethernet link. After a certain number of Ethernet frames are securely transmitted across the Ethernet link, MACsec automatically rotates to a new security association with a new security association number and key to maintain the secured Ethernet link. This rotation continues each time a certain number of Ethernet frames are securely transmitted across the secured Ethernet link, so you must always configure MACsec to have at least two security associations.</p> |
| <b>Default</b>                  | No security keys are configured, by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                  | <p><b><i>security-association-number</i></b>—Specifies the security association number and creates the SAK.</p> <p>The security association number is a whole number between 0 and 3. You can configure two security associations in a secure channel when enabling MACsec using static security keys.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## security-mode

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>security-mode <i>security-mode</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit security <b>macsec</b> <b>connectivity-association</b> <i>connectivity-association-name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 13.2X50-D15.</p> <p>The <b>dynamic</b> security mode option was introduced in Junos OS Release 14.1X53-D10.</p> <p>Statement introduced in Junos OS Release 14.1X53-D15 for the QFX Series.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Description</b>              | <p>Configure the MACsec security mode for the connectivity association.</p> <p>We recommend enabling MACsec on switch-to-switch Ethernet links using static connectivity association key (CAK) security mode. Static CAK security mode ensures security by frequently refreshing to a new random secure association key (SAK) and by only sharing the SAK between the two devices on the MACsec-secured point-to-point link. Additionally, some optional MACsec features—replay protection, SCI tagging, and the ability to exclude traffic from MACsec—are only available when you enable MACsec using static CAK security mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Options</b>                  | <p><b><i>security-mode</i></b>—Specifies the MACsec security mode. Options include:</p> <ul style="list-style-type: none"><li>• <b>dynamic</b>—Dynamic mode.</li></ul> <p>Dynamic security mode is used to enable MACsec on switch-to-host Ethernet links. In dynamic mode, a master key is retrieved from a RADIUS server by a switch and a host as part of the AAA handshake in separate transactions. The MKA protocol is enabled when the master key is exchanged between the switch and the host.</p> <ul style="list-style-type: none"><li>• <b>static-cak</b>—Static connectivity association key (CAK) mode.</li></ul> <p>Static CAK security mode is used to enable MACsec on switch-to-switch Ethernet links. In <b>static-cak</b> mode, the switch at one end of the point-to-point link acts as the key server and regularly transmits a randomized key using a process that does not transmit any traffic outside of the MACsec-secured point-to-point link.</p> <ul style="list-style-type: none"><li>• <b>static-sak</b>—Static secure association key (SAK) mode.</li></ul> <p>Static SAK security mode is used to enable MACsec on switch-to-switch Ethernet links. In <b>static-sak</b> mode, one of two user-configured security keys is used to secure the point-to-point link. The two security keys are regularly rotated.</p> |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## transmit-interval (MACsec)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>transmit-interval <i>interval</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | [edit security <b>macsec</b> <b>connectivity-association</b> <i>connectivity-association-name</i> mka]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Statement introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | <p>Specifies the transmit interval for MACsec Key Agreement (MKA) protocol data units (PDUs).</p> <p>The MKA transmit interval setting sets the frequency for how often the MKA PDU is sent to the directly connected device to maintain MACsec on a point-to-point Ethernet link. A lower <i>interval</i> increases bandwidth overhead on the link; a higher <i>interval</i> optimizes the MKA protocol data unit exchange process.</p> <p>The transmit interval settings must be identical on both ends of the link when MACsec using static connectivity association key (CAK) security mode is enabled.</p> <p>We recommend increasing the interval to 6000 ms in high-traffic load environments.</p> |
| <b>Default</b>                  | The default transmit interval is 2000 milliseconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                  | <i>interval</i> —Specifies the transmit interval, in milliseconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Media Access Control Security (MACsec) on page 99</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |





## CHAPTER 12

# Configuration Statements for Port Security

- `circuit-id` on page 244
- `dhcp-snooping-file` on page 245
- `fc-map` on page 246
- `fcoe-trusted` on page 248
- `mac-move-limit` on page 249
- `no-allowed-mac-log` on page 250
- `no-gratuitous-arp-request` on page 251
- `persistent-learning` on page 251
- `port-error-disable` on page 252
- `vendor-id` on page 254
- `write-interval` on page 255

## circuit-id

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> circuit-id {   prefix {     host-name;     logical-system-name;     routing-instance-name;   }   use-interface-description (device   logical);   use-vlan-id; } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | <ul style="list-style-type: none"> <li>For platforms with Enhanced Layer 2 Software (ELS):<br/>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82 ]</li> <li>For platforms without ELS:<br/>[edit ethernet-switching-options secure-access-port vlan (all   <i>vlan-name</i>) dhcp-option82],<br/>[edit forwarding-options helpers bootp dhcp-option82] ,<br/>[edit forwarding-options helpers bootp interface <i>interface-name</i> dhcp-option82]</li> <li>For MX Series platforms:<br/>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82]</li> </ul> |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Hierarchy level [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 14.1 for the MX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>                                                                                |
| <b>Description</b>              | <p>Configure the <b>circuit-id</b> suboption (suboption 1) of DHCP option 82 (the DHCP relay agent information option) in DHCP packets destined for a DHCP server. This suboption identifies the circuit (the interface, the VLAN, or both) on which the DHCP request arrived.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                         |
| <b>Default</b>                  | <p>If DHCP option 82 is enabled on the switch, the circuit ID is supplied by default in the format <i>interface-name:vlan-name</i> or, on a Layer 3 interface, just <i>interface-name</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b> | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><i>Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)</i></li> <li><i>Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server</i></li> <li><i>Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server</i></li> </ul>                                                                                                                                                                                                                                                 |

- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- *Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- RFC 3046, *DHCP Relay Agent Information Option*, at <http://tools.ietf.org/html/rfc3046>

## dhcp-snooping-file

|                                 |                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>dhcp-snooping-file {     location <i>local_pathname</i>   <i>remote_URL</i>;     timeout <i>seconds</i>;     write-interval <i>seconds</i>; }</pre>                                |
| <b>Hierarchy Level</b>          | <p>For platforms without ELS:</p> <pre>[edit ethernet-switching-options secure-access-port]</pre> <p>For platforms with ELS:</p> <pre>[edit system processes] dhcp-service ]</pre>      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1 for the QFX Series.                                                                                                                       |
| <b>Description</b>              | <p>Specify a local pathname or remote URL for the DHCP snooping database file to maintain persistence of IP-MAC bindings.</p> <p>The remaining statements are explained separately.</p> |
| <b>Default</b>                  | The IP-MAC bindings in the DHCP snooping database file are not persistent. If the switch is rebooted, the bindings are lost.                                                            |
| <b>Required Privilege Level</b> | <p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>                                                          |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Understanding DHCP Snooping for Port Security on page 124</a></li> </ul>                                                           |

## fc-map

**Syntax** `fc-map fc-map-value;`

**Hierarchy Level** Original CLI

[edit ethernet-switching options secure-access-port vlan (all | *vlan-name*) examine-fip]

ELS CLI for Platforms that Support FCoE

[edit vlans *vlan-name* forwarding-options fip-security]



**NOTE:** The `fc-map` configuration statement is in a different hierarchy on the original CLI than on the Enhanced Layer 2 Software (ELS) CLI.

QFX Series that Support FCoE-FC Gateway Configuration

[edit fc-fabrics *fc-fabric-name* protocols fip]

**Release Information** Statement introduced in Junos OS Release 10.4 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.  
Statement introduced for the ELS CLI in Junos OS Release 13.2 for the QFX Series.

**Description** Set the FCoE mapped address prefix (FC-MAP) value for the FCoE VLAN to match the FC switch (or FCoE forwarder) FC-MAP value for the FC fabric. The FC-MAP value is a unique MAC address prefix an FC switch uses to identify FCoE traffic for a given FC fabric (traffic on a particular FCoE VLAN).

You can configure the FC-MAP value or use the default value. The default FC-MAP value is different for VN\_Port to VF\_Port (VN2VF\_Port) FIP snooping (0x0EFC00) than for VN\_Port to VN\_Port (VN2VN\_Port) FIP snooping.

The FC switch provides the FC-MAP value to FCoE nodes (ENodes) in the FIP discovery advertisement message. If the EX Series switch or the QFX Series FCoE VLAN FC-MAP value does not match the FC switch FC-MAP value, neither device discovers the FC switch on that VLAN, and the ENodes on that VLAN cannot access the FC switch. The FC switch accepts only FCoE traffic that uses the correct FC-MAP value as part of the VN\_Port MAC address.

When the QFX Series acts as an FCoE-FC gateway, the FC-MAP value for the gateway and the FCoE devices must match the FC switch FC-MAP value in order to communicate with the FC switch.



**NOTE:** Changing the FC-MAP value causes all logins to drop and forces the ENodes to log in again.

**Options** `fc-map-value`—FC-MAP value, hexadecimal value preceded by "0x".

**Range:** 0x0EFC00 through 0x0EFCFF

**Default:** 0x0EFC00 for VN2VF\_Port FIP snooping 0x0EFD00 for VN2VN\_Port FIP snooping

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

**Related Documentation**

- *examine-fip*
- *show fip snooping*
- *Example: Configuring an FCoE Transit Switch*
- *Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

## fcoe-trusted

**Syntax** `fcoe-trusted;`

**Hierarchy Level** Original CLI

[edit ethernet-switching-options secure-access-port interface *interface-name*]

ELS CLI for Platforms that Support FCoE

[edit vlans *vlan-name* forwarding-options fip-security interface *interface-name*]



**NOTE:** The `fcoe-trusted` configuration statement is in a different hierarchy on the original CLI than on the Enhanced Layer 2 Software (ELS) CLI.

QFX Series that Support FCoE-FC Gateway Configuration

[edit fc-fabrics *fc-fabric-name* protocols fip]

**Release Information** Statement introduced in Junos OS Release 10.4 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.  
Statement introduced for the FC fabric in Junos OS Release 11.3 for the QFX Series.  
Statement introduced for the ELS CLI in Junos OS Release 13.2 for the QFX Series.

**Description** Configure the specified 10-Gigabit Ethernet interface to trust Fibre Channel over Ethernet (FCoE) traffic. If an interface is connected to another switch such as an FCoE forwarder (FCF) or a transit switch, you can configure the interface as trusted so that the interface forwards FCoE traffic from the switch to the FCoE devices without installing FIP snooping filters.


(QFX Series FCoE-FC gateway) Configure the specified local Fibre Channel fabric to trust FCoE traffic on all ports in the fabric. Changing the fabric ports from untrusted to trusted removes any existing FIP snooping filters from the ports. Changing the fabric ports from trusted to untrusted by removing the **fcoe-trusted** configuration from the fabric forces all of the FCoE sessions on those ports to log out so that when the ENodes and VN\_Ports log in again, the switch can build the appropriate FIP snooping filters.

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

**Related Documentation**

- *show fip snooping*
- *Example: Configuring an FCoE Transit Switch*
- *Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*
- *Configuring VN2VF\_Port FIP Snooping and FCoE Trusted Interfaces on an FCoE Transit Switch*

## mac-move-limit

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>mac-move-limit <i>limit</i> &lt;fabric-limit <i>limit</i>&gt; action <i>action</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | <p>For platforms without ELS:</p> <pre>[edit ethernet-switching-options secure-access-port (all   <i>vlan-name</i>)]</pre> <p>For platforms with ELS:</p> <pre>[edit vlans <i>vlan-name</i> switch-options],</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1 for the QFX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>              | Specify the number of times a MAC address can move to a new interface (port) in 1 second and the action to be taken by the switch if the MAC address move limit is exceeded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                                 | <div>  <p><b>CAUTION:</b> Mac move limiting does not work properly on a QFX5100 switch used as a Node device in a QFabric system. Do not use this feature on a QFX5100 switch in a QFabric system.</p> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Default</b>                  | The default move limit is unlimited. The default action is <b>drop</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Options</b>                  | <p><b>fabric-limit</b>—Specify the maximum number of moves in a QFabric system. If you do not specify a fabric limit, the value for <b>mac-move-limit</b> applies to the QFabric system.</p> <p><b>limit</b>—Maximum number of moves to a new interface per second.</p> <p><b>action <i>action</i></b>—(Optional) Action to take when the MAC address move limit is reached:</p> <ul style="list-style-type: none"> <li>• <b>drop</b>—Drop the packet and generate an alarm, an SNMP trap, or a system log entry. This is the default.</li> <li>• <b>log</b>—Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry.</li> <li>• <b>none</b>—No action.</li> <li>• <b>shutdown</b>—Logically disable the interface and generate a system log entry. If you have configured the switch with the <b>port-error-disable</b> statement, the disabled interfaces recover automatically upon expiration of the specified disable timeout. If you have not configured the switch for autorecovery from port error disabled conditions, you can bring up the disabled interfaces by running the <b>clear-ethernet-switch-port</b> command.</li> </ul> |
| <b>Required Privilege Level</b> | <p>system—To view this statement in the configuration.</p> <p>system—control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

- Related Documentation**
- *mac-limit*
  - *Example: Configuring Basic Port Security Features*
  - *Configuring MAC Move Limiting (CLI Procedure)*
  - *Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)*

---

## no-allowed-mac-log

---

- Syntax** no-allowed-mac-log;
- Hierarchy Level**
- For platforms without ELS:  
[edit ethernet-switching-options secure-access-port interface (all | *interface-name*)]
  - For platforms with ELS:  
[edit switch-options interface *interface-name*]
- Release Information** Statement introduced in Junos OS Release 11.1 for the QFX Series.
- Description** Specify that the switch should not log messages when it receives packets from invalid MAC addresses on an interface that has been configured for allowed MAC addresses.
- Default** The switch logs messages when it receives packets from invalid MAC addresses on an interface that has been configured for particular allowed (specific) MAC addresses.
- Required Privilege Level**
- routing—To view this statement in the configuration.  
routing—control—To add this statement to the configuration.
- Related Documentation**
- [Understanding MAC Limiting and MAC Move Limiting for Port Security on page 135](#)
  - *Configuring MAC Limiting*
  - *allowed-mac*
  - *mac-limit*




## no-gratuitous-arp-request

|                                 |                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | no-gratuitous-arp-request;                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> ],<br>[edit interfaces interface-range <i>interface-name</i> ]                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                     |
| <b>Description</b>              | Configure the switch not to respond to gratuitous ARP requests. You can disable responses to gratuitous ARP requests on both Layer 2 Ethernet switching interfaces and routed VLAN interfaces (RVIs). |
| <b>Default</b>                  | Gratuitous ARP responses are enabled on all Ethernet switching interfaces and RVIs.                                                                                                                   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                               |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Configuring IRB Interfaces</i></li> </ul>                                                                                                                 |

## persistent-learning

|                                 |                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | persistent-learning;                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | <ul style="list-style-type: none"> <li>• For platforms without ELS:<br/>[edit ethernet-switching-options secure-access-port interface (all   <i>interface-name</i>)]</li> <li>• For platforms with ELS:<br/>[edit switch-options interface <i>interface-name</i>]</li> </ul> |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.4 for EX Series switches.<br>Statement introduced in Junos OS Release 12.1 for the QFX Series.<br>Hierarchy level [edit switch-options interface <i>interface-name</i> ] introduced in Junos OS Release 13.2X50-D10              |
| <b>Description</b>              | Specify that learned MAC addresses persist on the specified interfaces across restarts of the switch and link-down conditions. This feature is also known as sticky MAC.                                                                                                     |
| <b>Required Privilege Level</b> | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Example: Configuring Basic Port Security Features</i></li> <li>• <i>Configuring Persistent MAC Learning (CLI Procedure)</i></li> <li>• <i>Configuring Persistent MAC Learning (CLI Procedure)</i></li> </ul>                     |

## port-error-disable

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>port-error-disable {   (disable-timeout <i>seconds</i>   recovery-timeout <i>seconds</i>); }</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | <ul style="list-style-type: none"> <li>For platforms without ELS:<br/>[edit ethernet-switching-options]</li> <li>For platforms with ELS:<br/>[edit switch-options ]</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 on the QFX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | Disable rather than block an interface when enforcing MAC limiting, MAC move limiting, and storm control, and allow the interface to recover automatically from the error condition after a specified period of time:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                                 | <p> <b>NOTE:</b> The <b>port-error-disable</b> configuration does not apply to preexisting error conditions. It affects only error conditions that are detected after you enable and commit the <b>port-error-disable</b> statement. To clear a preexisting error condition and restore the interface to service, use the <a href="#">clear ethernet-switching port-error</a> command.</p> <ul style="list-style-type: none"> <li>If you enable the <i>mac-limit</i> statement with the <b>shutdown</b> option and also enable the <b>port-error-disable</b> statement, the switch disables (rather than shuts down) the interface when the MAC address limit is reached.</li> <li>If you have enabled the <a href="#">mac-move-limit</a> statement with the <b>shutdown</b> option and you enable the <b>port-error-disable</b> statement, the switch disables (rather than shuts down) the interface when the maximum number of moves to a new interface is reached.</li> <li>If you enable the <i>storm-control</i> statement with the <b>action-shutdown</b> option and you also enable <b>port-error-disable</b>, the switch disables (rather than shuts down) the interface when broadcast traffic and unknown unicast traffic exceed the specified levels.</li> </ul> |
| <b>Default</b>                  | Not enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing—control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">Understanding MAC Limiting and MAC Move Limiting for Port Security on page 135</a></li> <li><a href="#">Understanding Storm Control on page 151</a></li> <li><a href="#">Example: Configuring Storm Control to Prevent Network Outages</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

- *Configuring Autorecovery for MAC Limited or Storm Control Interfaces (CLI Procedure)*
- [action-shutdown on page 258](#)
- *disable-timeout*
- [clear ethernet-switching port-error on page 314](#)

## vendor-id

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                             | <code>vendor-id &lt;string&gt;;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>For Platforms with Enhanced Layer 2 Software (ELS)</b> | [edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>For Platforms Without ELS</b>                          | [edit ethernet-switching-options secure-access-port vlan (all   <i>vlan-name</i> ) dhcp-option82],<br>[edit forwarding-options helpers bootp dhcp-option82],<br>[edit forwarding-options helpers bootp interface <i>interface-name</i> dhcp-option82]                                                                                                                                                                                                                                                                                                                                                 |
| <b>For MX Series Platforms</b>                            | [edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>                                | Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 11.3 for the QFX Series.<br>Hierarchy level [edit vlans <i>vlan-name</i> forwarding-options dhcp-security] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)<br>Hierarchy level [edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security] introduced in Junos OS Release 14.1 for the MX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. |
| <b>Description</b>                                        | Insert a vendor ID in the DHCP option 82 information in a DHCP request packet header before forwarding or relaying the request to a DHCP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Default</b>                                            | If <b>vendor-id</b> is not explicitly configured for DHCP option 82, then no vendor ID is set.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Options</b>                                            | <b>string</b> —(Optional) A single string that designates the vendor ID.<br><br><b>Range:</b> 1–255 characters<br><br><b>Default:</b> If you specify <b>vendor-id</b> with no <b>string</b> value, then the default vendor ID <b>Juniper Networks</b> is configured.                                                                                                                                                                                                                                                                                                                                  |
| <b>Required Privilege Level</b>                           | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>                              | <ul style="list-style-type: none"> <li>• <i>Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)</i></li> <li>• <i>Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server</i></li> <li>• <i>Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server</i></li> <li>• <i>Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)</i></li> </ul>                                                                                              |

---

## write-interval

---

|                                 |                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>write-interval <i>seconds</i>;</code>                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | For platforms without ELS:<br><br>[edit ethernet-switching-options secure-access-port <a href="#">dhcp-snooping-file</a> ]<br><br>For platforms with ELS:<br><br>[edit system processes] dhcp-service dhcp-snooping-file] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.1 for the QFX Series.                                                                                                                                                         |
| <b>Description</b>              | Specify how frequently the switch writes the database entries from memory into the specified DHCP snooping database file.                                                                                                 |
| <b>Default</b>                  | None                                                                                                                                                                                                                      |
| <b>Options</b>                  | <i>seconds</i> —Value in seconds.<br><b>Range:</b> 60 through 86400                                                                                                                                                       |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Understanding DHCP Snooping for Port Security on page 124</a></li></ul>                                                                                               |




## CHAPTER 13

# Configuration Statements for Device Security

- [action-shutdown on page 258](#)
- [bandwidth-level on page 259](#)
- [bandwidth-percentage on page 260](#)
- [interface \(Unknown Unicast Forwarding\) on page 261](#)
- [no-broadcast on page 262](#)
- [no-multicast on page 263](#)
- [no-unknown-unicast on page 264](#)
- [rpf-check on page 265](#)
- [storm-control on page 266](#)
- [storm-control-profiles on page 267](#)
- [unknown-unicast-forwarding on page 268](#)


## action-shutdown

---


|                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                  | action-shutdown;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>                                                                                                                                                                                         | For platforms without ELS:<br><br>[edit ethernet-switching-options storm-control]<br><br>For platforms with ELS:<br><br>[edit forwarding-options <a href="#">storm-control-profiles</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Release Information</b>                                                                                                                                                                                     | Statement introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>                                                                                                                                                                                             | <p>Shut down or disable interfaces when the storm control level is exceeded, as follows:</p> <ul style="list-style-type: none"><li>• If you set both the <b>action-shutdown</b> and the <b>port-error-disable</b> statements, the affected interfaces are disabled temporarily and recover automatically when the disable timeout expires.</li><li>• If you set the <b>action-shutdown</b> statement and do not set the <b>port-error-disable</b> statement, the affected interfaces are shut down when the storm control level is exceeded, and they do not recover automatically. You must issue the <b>clear ethernet-switching port-error</b> command to clear the port error and restore the interfaces to service.</li></ul> |
| <div> <b>NOTE:</b> This statement is not supported for OVSDB-managed interfaces on which storm control is configured.</div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Default</b>                                                                                                                                                                                                 | The <b>action-shutdown</b> feature is disabled. If the storm control level is exceeded, the switch drops broadcast and unknown unicast messages on the specified interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Required Privilege Level</b>                                                                                                                                                                                | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>                                                                                                                                                                                   | <ul style="list-style-type: none"><li>• <a href="#">Understanding Storm Control on page 151</a></li><li>• <i>Example: Configuring Storm Control to Prevent Network Outages</i></li><li>• <a href="#">port-error-disable on page 252</a></li><li>• <i>disable-timeout</i></li><li>• <a href="#">clear ethernet-switching port-error on page 314</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                       |



## bandwidth-level

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <code>bandwidth-level <i>kbps</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | [edit forwarding-options <a href="#">storm-control-profiles</a> <i>profile-name</i> all]                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.<br>Statement introduced in Junos OS Release 13.2 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1 for MX Series routers.                                                                                                                                                                                                                                        |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Configure the storm control level as the bandwidth in kilobits per second of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams.                                                                                                                                                                                                                                                                             |
| <div>  <p><b>NOTE:</b> When you configure storm control level on an aggregated Ethernet interface, the storm control level for each member of the aggregated Ethernet interface is set to that bandwidth. For example, if you configure a storm control level of 15,000 Kbps on ae1, and ae1 has two members, ge-0/0/0 and ge-0/0/1, each member has a storm control level of 15,000 Kbps. Thus, the storm control level on ae1 allows a traffic rate of up to 30,000 Kbps of combined broadcast, multicast, and unknown unicast traffic.</p> </div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Default</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p>On EX4300 switches—If you do not specify the storm control level using either the <b>bandwidth-level</b> or the <b>bandwidth-percentage</b> statements, the storm control level defaults to 80 percent of the available bandwidth used by the combined broadcast, unknown unicast, and multicast traffic streams.</p> <p>On EX9200 switches—Storm control is not enabled by default.</p> <p>On MX Series routers—Storm control is not enabled by default.</p> |
| <b>Options</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p><b>bandwidth-level <i>kbps</i></b>—Traffic rate in kilobits per second of the combined broadcast, multicast, and unknown unicast traffic streams.</p> <p><b>Range:</b> 100 through 10,000,000</p> <p><b>Default:</b> None</p>                                                                                                                                                                                                                                 |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                     |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>• <a href="#">bandwidth-percentage on page 260</a></li> <li>• <i>Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches</i></li> <li>• <i>Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers</i></li> <li>• <i>Configuring or Disabling Storm Control (CLI Procedure)</i></li> </ul>                                                                         |

## bandwidth-percentage

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <code>bandwidth-percentage <i>percentage</i>;</code>                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | [edit forwarding-options <a href="#">storm-control-profiles</a> <i>profile-name</i> all]                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.<br>Statement introduced in Junos OS Release 13.2 for the QFX series.<br>Statement introduced in Junos OS Release 14.1 for MX Series routers.                                                                                                                                                           |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Configure the storm control level as the percentage of available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams on an interface.<br>The storm control level is configured as part of the storm control profile.                                                                                                                           |
| <div>  <p><b>NOTE:</b> When you configure storm control level on an aggregated Ethernet interface, the storm control level for each member of the aggregated Ethernet interface is set to that bandwidth. For example, if you configure a storm control level of 15,000 Kbps on ae1, and ae1 has two members, ge-0/0/0 and ge-0/0/1, each member has a storm control level of 15,000 Kbps. Thus, the storm control level on ae1 allows a traffic rate of up to 30,000 Kbps of combined broadcast, multicast, and unknown unicast traffic.</p> </div> |                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Default</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <p>On EX4300 switches—The storm control level is 80 percent of the available bandwidth used by the combined broadcast, unknown unicast, and multicast traffic streams.</p> <p>On EX9200 switches—Storm control is not enabled by default.</p> <p>On MX Series routers—Storm control is not enabled by default.</p>                                                                  |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>• <a href="#">bandwidth-level on page 259</a></li> <li>• <i>Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches</i></li> <li>• <i>Example: Configuring Storm Control to Prevent Network Outages on MX Series Routers</i></li> <li>• <i>Configuring or Disabling Storm Control (CLI Procedure)</i></li> </ul> |

## interface (Unknown Unicast Forwarding)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>interface <i>interface-name</i>;</code>                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Hierarchy Level</b>          | <ul style="list-style-type: none"> <li>For platforms with ELS:<br/>[edit switch-options <b>unknown-unicast-forwarding</b> vlan <i>vlan-name</i>]</li> <li>For platforms without ELS:<br/>[edit ethernet-switching-options <b>unknown-unicast-forwarding</b> vlan <i>vlan-name</i>]</li> </ul>                                                                                                                               |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> <p>Hierarchy level <b>[edit switch-options]</b> introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> |
| <b>Description</b>              | Specify the interface to which unknown unicast packets will be forwarded.                                                                                                                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b> | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><code>show vlans</code></li> <li><code>show ethernet-switching table</code></li> <li><i>Configuring Unknown Unicast Forwarding (CLI Procedure)</i></li> <li><a href="#">Understanding Unknown Unicast Forwarding on page 157</a></li> </ul>                                                                                                                                          |

## no-broadcast

---

|                                 |                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | no-broadcast;                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | For platforms without ELS:<br><br>[edit ethernet-switching-options storm-control interface (all   <i>interface-name</i> )]<br><br>For platforms with ELS:<br><br>[edit forwarding-options <a href="#">storm-control-profiles</a> ] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                      |
| <b>Description</b>              | For interfaces configured for storm control, disable broadcast traffic storm control on the interface.                                                                                                                             |
| <b>Default</b>                  | When storm control is enabled on an interface, it is enabled for broadcast traffic (as well as multicast and unknown unicast traffic).                                                                                             |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Understanding Storm Control on page 151</a></li><li>• <i>Example: Configuring Storm Control to Prevent Network Outages</i></li></ul>                                           |

## no-multicast

---

|                                 |                                                                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | no-multicast;                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | <p>For platforms without ELS:</p> <p>[edit ethernet-switching-options storm-control interface (all   <i>interface-name</i>)]</p> <p>For platforms with ELS:</p> <p>[edit forwarding-options <a href="#">storm-control-profiles</a>]</p> |
| <b>Release Information</b>      | <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>                                                                                |
| <b>Description</b>              | Disable storm control for all multicast traffic (both registered multicast and unregistered multicast) for the specified interface or for all interfaces.                                                                               |
| <b>Default</b>                  | Storm control is enabled for unknown unicast traffic, multicast traffic, and broadcast traffic.                                                                                                                                         |
| <b>Required Privilege Level</b> | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>                                                                                                            |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Understanding Storm Control on page 151</a></li> <li>• <i>Example: Configuring Storm Control to Prevent Network Outages</i></li> </ul>                                             |

## no-unknown-unicast

---


|                                 |                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | no-unknown-unicast;                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | For platforms without ELS:<br><br>[edit ethernet-switching-options storm-control interface (all   <i>interface-name</i> )]<br><br>For platforms with ELS:<br><br>[edit forwarding-options <a href="#">storm-control-profiles</a> ] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.1 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                      |
| <b>Description</b>              | For interfaces configured for storm control, disable unknown unicast traffic storm control on the interface.                                                                                                                       |
| <b>Default</b>                  | When storm control is enabled on an interface, it is enabled for both unknown unicast traffic and broadcast traffic.                                                                                                               |
| <b>Required Privilege Level</b> | routing—To view this statement in the configuration.<br>routing-control—To add this statement to the configuration.                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Understanding Storm Control on page 151</a></li><li>• <i>Example: Configuring Storm Control to Prevent Network Outages</i></li></ul>                                           |

## rpf-check

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | rpf-check;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>          | [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet],<br>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet6]                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 9.3 for EX Series switches.<br>Statement introduced in Junos OS Release 13.2 for the QFX Series.<br>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | <p>On EX3200 and EX4200 switches, enable a reverse-path forwarding (RPF) check on unicast traffic (except ECMP packets) on all ingress interfaces.</p> <p>On EX4300 switches, enable a reverse-path forwarding (RPF) check on unicast traffic, including ECMP packets, on all ingress interfaces.</p> <p>On EX8200 and EX6200 switches, enable an RPF check on unicast traffic, including ECMP packets, on the selected ingress interfaces.</p> <p>On QFX Series switches, enable an RPF check on unicast traffic (except ECMP packets) on the selected ingress interfaces.</p> |
| <b>Default</b>                  | Unicast RPF is disabled on all interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Example: Configuring Unicast RPF on an EX Series Switch</i></li> <li>• <a href="#">Configuring Unicast RPF (CLI Procedure) on page 160</a></li> <li>• <a href="#">Disabling Unicast RPF (CLI Procedure) on page 162</a></li> <li>• <a href="#">Understanding Unicast RPF on page 153</a></li> </ul>                                                                                                                                                                                                                                 |

## storm-control

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <code>storm-control storm-control-profile;</code>                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | [edit interfaces <i>interface-name</i> unit <i>number</i> family ethernet-switching],<br>[edit interfaces <i>interface-name</i> unit <i>number</i> family bridge]<br>[edit interfaces <i>interface-name</i> ether-options ethernet-switch-profile]                                                                                                 |
| <b>Release Information</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.<br>Statement introduced in Junos OS Release 13.2 for the QFX series.<br>Statement introduced in Junos OS Release 14.1 for the MX Series routers.                                                                                                                      |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <p>Bind a storm control profile to a logical interface.</p> <p>On switches running ELS software, storm control is enabled by default on all switch interfaces at a level of 80 percent of the combined broadcast and unknown unicast streams. (For the equivalent statement for platforms running non-ELS software, see <i>storm-control</i>.)</p> |
| <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p><b>NOTE:</b> If you configure storm control on an aggregated Ethernet interface, the storm-control level is applied to each member interface individually. For example, if the aggregated interface has two members and you configure a storm-control level of 20 kbps, Junos will not detect a storm if one or both of the member interfaces receives traffic at 15 kbps because in neither of these cases does an individual member receive traffic at a rate greater than the configured storm-control level. In this example, Junos detects a storm only if at least one member interface receives traffic at greater than 20 Kbps.</p> </div> </div> |                                                                                                                                                                                                                                                                                                                                                    |
| <b>Required Privilege Level</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | system—To view this statement in the configuration.<br>system-control—To add this statement to the configuration.                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• <i>Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches</i></li> <li>• <i>Understanding Storm Control on Switching Devices</i></li> </ul>                                                                                                                                  |



## storm-control-profiles

|                                 |                                                                                                                                                                                                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>storm-control-profiles <i>profile-name</i> {   action-shutdown;   all {     bandwidth-level;     bandwidth-percentage;     no-broadcast;     no-multicast;     no-registered-multicast;     no-unknown-unicast;     no-unregistered-multicast;   } }</pre> |
| <b>Hierarchy Level</b>          | [edit forwarding-options]                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1 for MX Series routers.</p>                        |
| <b>Description</b>              | <p>Configure a storm control profile on a switch or router.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                       |
| <b>Required Privilege Level</b> | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches</i></li> <li>• <i>Understanding Storm Control on Switching Devices</i></li> </ul>                                               |

## unknown-unicast-forwarding

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>unknown-unicast-forwarding {<br/>  vlan <i>vlan-name</i> {<br/>    interface <i>interface-name</i>;<br/>  }<br/>}</pre>                                                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | <ul style="list-style-type: none"><li>• For platforms with ELS:<br/>[edit switch-options]</li><li>• For platforms without ELS:<br/>[edit ethernet-switching-options]</li></ul>                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 9.3 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX Series.</p> <p>Hierarchy level [edit switch-options] introduced in Junos OS Release 13.2X50-D10. (See <i>Getting Started with Enhanced Layer 2 Software</i> for information about ELS.)</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> |
| <b>Description</b>              | <p>Configure the switch to forward all unknown unicast packets in a VLAN or on all VLANs to a particular interface.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                    |
| <b>Default</b>                  | Unknown unicast packets are flooded to all interfaces that belong to the same VLAN.                                                                                                                                                                                                                                                                                                                                  |
| <b>Required Privilege Level</b> | <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>show vlans</i></li><li>• <i>show ethernet-switching table</i></li><li>• <a href="#">Configuring Unknown Unicast Forwarding (CLI Procedure) on page 165</a></li><li>• <a href="#">Understanding Unknown Unicast Forwarding on page 157</a></li></ul>                                                                                                                       |


## CHAPTER 14

# Configuration Statements for DDoS Protection


- [bandwidth \(DDoS\) on page 270](#)
- [bandwidth-scale \(DDoS\) on page 271](#)
- [burst \(DDoS\) on page 272](#)
- [burst-scale \(DDoS\) on page 273](#)
- [ddos-protection \(DDoS\) on page 274](#)
- [disable-fpc \(DDoS\) on page 275](#)
- [disable-logging \(DDoS\) on page 276](#)
- [disable-routing-engine \(DDoS\) on page 277](#)
- [fpc \(DDoS\) on page 278](#)
- [global \(DDoS\) on page 279](#)
- [protocols \(DDoS\) on page 280](#)
- [recover-time \(DDoS\) on page 283](#)
- [traceoptions \(DDoS\) on page 284](#)

## bandwidth (DDoS)


---

|                                                                                                                                                                       |                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                         | <code>bandwidth <i>packets-per-second</i>;</code>                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>                                                                                                                                                | [edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> )]                                                                                                                                                                           |
| <b>Release Information</b>                                                                                                                                            | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                                                                                                              |
| <b>Description</b>                                                                                                                                                    | (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or QFX5100 switches) Configure the DDoS bandwidth rate limit; the maximum traffic rate (packets per second) allowed by the specified policer. When the value is exceeded, a violation is declared. |
| <div> <b>NOTE:</b> Packet-type policers are not supported on QFX5100 switches.</div> |                                                                                                                                                                                                                                                                           |
| <b>Options</b>                                                                                                                                                        | <i>packets-per-second</i> —Number of packets per second that are allowed by the aggregate or packet-type policer.<br><b>Range:</b> 1 through 100,000 packets per second                                                                                                   |
| <b>Required Privilege Level</b>                                                                                                                                       | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                           |
| <b>Related Documentation</b>                                                                                                                                          | <ul style="list-style-type: none"><li>• <a href="#">Configuring DDoS Protection Policers for Individual Packet Types</a></li><li>• <a href="#">Configuring DDoS Protection Policers on QFX Series Switches on page 174</a></li></ul>                                      |


## bandwidth-scale (DDoS)

|                                                                                                                                                                         |                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                           | <code>bandwidth-scale <i>percentage</i>;</code>                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>                                                                                                                                                  | [edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> ) <b>fpc</b> <i>slot-number</i> ]                                                                                                                                          |
| <b>Release Information</b>                                                                                                                                              | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                                                                                                            |
| <b>Description</b>                                                                                                                                                      | (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or QFX5100 switches) Configure the percentage by which the DDoS bandwidth rate limit is scaled down for the aggregate or packet-type policer on the card in the specified slot or on the switch. |
| <div>  <b>NOTE:</b> Packet-type policers are not supported on QFX5100 switches. </div> |                                                                                                                                                                                                                                                                         |
| <b>Options</b>                                                                                                                                                          | <p><b><i>percentage</i></b>—Percentage multiplied by the bandwidth rate limit to reduce the number of packets per second allowed for the packet type.</p> <p><b>Range:</b> 1 through 100 percent</p> <p><b>Default:</b> 100</p>                                         |
| <b>Required Privilege Level</b>                                                                                                                                         | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                              |
| <b>Related Documentation</b>                                                                                                                                            | <ul style="list-style-type: none"> <li>• <a href="#">Configuring DDoS Protection Policers for Individual Packet Types</a></li> <li>• <a href="#">Configuring DDoS Protection Policers on QFX Series Switches on page 174</a></li> </ul>                                 |

## burst (DDoS)

|                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                           | <code>burst size;</code>                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>                                                                                                                                                  | [edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> )]                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>                                                                                                                                              | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>                                                                                                                                                      | (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or QFX5100 switches) Configure the DDoS burst limit; the maximum number of packets that is allowed in a burst of traffic by the specified policer. When this value is exceeded, a violation is declared.                                                                                                                                               |
| <div>  <b>NOTE:</b> Packet-type policers are not supported on QFX5100 switches. </div> |                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                                                                                                                                                          | <p><b>size</b>—Number of packets that are allowed in a burst by the aggregate or packet-type policer.</p> <p><b>Range:</b> 1 through 100,000 packets</p> <p><b>Default:</b> The default burst value varies by packet type. You can view the default values for all packet types on an unconfigured router or switch by entering the <b>show ddos-protection protocols parameters brief</b> command from operational mode.</p> |
| <b>Required Privilege Level</b>                                                                                                                                         | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>                                                                                                                                            | <ul style="list-style-type: none"> <li><a href="#">Configuring DDoS Protection Policers for Individual Packet Types</a></li> <li><a href="#">Configuring DDoS Protection Policers on QFX Series Switches on page 174</a></li> </ul>                                                                                                                                                                                           |

## burst-scale (DDoS)

|                                                                                                                                                                         |                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                           | <code>burst-scale <i>percentage</i>;</code>                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>                                                                                                                                                  | [edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> ) <b>fpc</b> <i>slot-number</i> ]                                                                                                              |
| <b>Release Information</b>                                                                                                                                              | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                                                                                |
| <b>Description</b>                                                                                                                                                      | (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or QFX5100 switches) Configure the percentage by which the DDoS burst limit is scaled down for the aggregate or packet-type policer on the specified card or switch. |
| <div>  <b>NOTE:</b> Packet-type policers are not supported on QFX5100 switches. </div> |                                                                                                                                                                                                                                             |
| <b>Options</b>                                                                                                                                                          | <p><b>percentage</b>—Percentage multiplied by the burst limit to reduce the number of packets allowed in a burst for the packet type or protocol.</p> <p><b>Range:</b> 1 through 100 percent</p> <p><b>Default:</b> 100</p>                 |
| <b>Required Privilege Level</b>                                                                                                                                         | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                  |
| <b>Related Documentation</b>                                                                                                                                            | <ul style="list-style-type: none"> <li>Configuring DDoS Protection Policers for Individual Packet Types</li> <li>Configuring DDoS Protection Policers on QFX Series Switches on page 174</li> </ul>                                         |

## ddos-protection (DDoS)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> ddos-protection   global {     disable-fpc;     disable-logging;   }   protocols protocol-group aggregate {     bandwidth packets-per-second;     burst size;     disable-fpc;     disable-logging;     disable-routing-engine     fpc slot-number {       bandwidth-scale percentage;       burst-scale percentage;       disable-fpc;     }     recover-time   }   traceoptions {     file filename &lt;files number&gt; &lt;match regular-expression &gt; &lt;size maximum-file-size&gt;       &lt;world-readable   no-world-readable&gt;;     flag flag;     level (all   error   info   notice   verbose   warning);     no-remote-trace;   } } </pre> |
| <b>Hierarchy Level</b>          | [edit system]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Description</b>              | <p>Configure DDoS policers.</p> <p>The remaining statements are explained separately.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">Configuring DDoS Protection Policers on QFX Series Switches on page 174</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



## disable-fpc (DDoS)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | disable-fpc;                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>     | [edit system ddos-protection <a href="#">global</a> ],<br>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> )],<br>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> ) <a href="#">fpc</a><br><i>slot-number</i> ]                                                                                                                                         |
| <b>Release Information</b> | Statement introduced in Junos OS Release 11.2.<br>Support at the [edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> )] hierarchy level introduced in Junos OS Release 12.1.<br>Statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                                                                                                              |
| <b>Description</b>         | (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or QFX5100 switches) Disable DDoS policers for debugging purposes on the card in the specified slot for a particular packet type within a protocol group, on all cards for a particular packet type within a protocol group, or globally on all cards and for all packet types in all protocols. This statement does not affect the state of the Routing Engine policers. |




**NOTE:** Packet-type policers are not supported on QFX5100 switches.


|                                 |                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Disabling DDoS Protection Policers and Logging Globally on page 174</a></li> <li>• <a href="#">Configuring DDoS Protection Policers for Individual Packet Types</a></li> <li>• <a href="#">Configuring DDoS Protection Policers on QFX Series Switches on page 174</a></li> </ul> |

## disable-logging (DDoS)

---


|                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                         | disable-logging;                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>                                                                                                                                                | [edit system ddos-protection <a href="#">global</a> ],<br>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> )]                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>                                                                                                                                            | Statement introduced in Junos OS Release 11.2.<br>Support at the [edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> )] hierarchy level introduced in Junos OS Release 12.1.<br>Statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                                                                                               |
| <b>Description</b>                                                                                                                                                    | (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or QFX5100 switches) Disable router- or switch-wide logging of all DDoS violation and flow detection events globally. Disable only logging of events other than flow detection culprit flow events for a particular packet type within a protocol group. Typically used for debugging purposes.                                                            |
| <div> <b>NOTE:</b> Packet-type policers are not supported on QFX5100 switches.</div> |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Required Privilege Level</b>                                                                                                                                       | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>                                                                                                                                          | <ul style="list-style-type: none"><li>• <a href="#">Disabling DDoS Protection Policers and Logging Globally on page 174</a></li><li>• <a href="#">Configuring DDoS Protection Policers for Individual Packet Types</a></li><li>• <a href="#">Disabling Automatic Logging of Culprit Flow Events for a Packet Type</a></li><li>• <a href="#">Configuring DDoS Protection Policers on QFX Series Switches on page 174</a></li></ul> |

## disable-routing-engine (DDoS)

|                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                           | disable-routing-engine;                                                                                                                                                                                                                                                                                                             |
| <b>Hierarchy Level</b>                                                                                                                                                  | [edit system ddos-protection <a href="#">global</a> ],<br>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> )                                                                                                                                                                            |
| <b>Release Information</b>                                                                                                                                              | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                                                                                                                                                                        |
| <b>Description</b>                                                                                                                                                      | (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or QFX5100 switches) Disable DDoS Routing Engine policers for debugging purposes for a particular packet type within a protocol group or globally for all packet types in all protocols. This statement does not affect the state of the line card policers. |
| <div>  <b>NOTE:</b> Packet-type policers are not supported on QFX5100 switches. </div> |                                                                                                                                                                                                                                                                                                                                     |
| <b>Required Privilege Level</b>                                                                                                                                         | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                     |
| <b>Related Documentation</b>                                                                                                                                            | <ul style="list-style-type: none"> <li>• <a href="#">Disabling DDoS Protection Policers and Logging Globally on page 174</a></li> </ul>                                                                                                                                                                                             |

## fpc (DDoS)

---

|                                                                                                                                                                       |                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                         | <pre>fpc slot-number;<br/>    bandwidth-scale percentage;<br/>    burst-scale percentage;<br/>    disable-fpc;<br/>}</pre>                                                                                                           |
| <b>Hierarchy Level</b>                                                                                                                                                | [edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> )]                                                                                                                                      |
| <b>Release Information</b>                                                                                                                                            | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                                                                         |
| <b>Description</b>                                                                                                                                                    | (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or QFX5100 switches) Modify the DDoS aggregate or packet-type policer on the specified card or on the switch.                                                 |
| <div> <b>NOTE:</b> Packet-type policers are not supported on QFX5100 switches.</div> |                                                                                                                                                                                                                                      |
| <b>Options</b>                                                                                                                                                        | <p><b>slot-number</b>—Slot number of the card or FPC on the switch.</p> <p><b>Range:</b> Depends on the router or switch model</p> <p>The remaining statements are explained separately.</p>                                         |
| <b>Required Privilege Level</b>                                                                                                                                       | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                      |
| <b>Related Documentation</b>                                                                                                                                          | <ul style="list-style-type: none"><li>• <a href="#">Configuring DDoS Protection Policers for Individual Packet Types</a></li><li>• <a href="#">Configuring DDoS Protection Policers on QFX Series Switches on page 174</a></li></ul> |

---

## global (DDoS)

---

|                                 |                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>global {<br/>  disable-fpc;<br/>  disable-logging;<br/>  disable-routing-engine;<br/>  flow-detection;<br/>  flow-report-rate;<br/>  violation-report-rate;<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit system ddos-protection]                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.<br>Statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                 |
| <b>Description</b>              | Modify DDoS policers, event logging, and flow detection globally for all protocols.<br><br>The remaining statements are explained separately.                                |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Disabling DDoS Protection Policers and Logging Globally on page 174</a></li></ul>                                        |

## protocols (DDoS)

---

**Syntax**    `protocols protocol-group aggregate {  
                  bandwidth packets-per-second;  
                  burst size;  
                  disable-fpc;  
                  disable-logging;  
                  disable-routing-engine  
                  fpc slot-number {  
                      bandwidth-scale percentage;  
                      burst-scale percentage;  
                      disable-fpc;  
                  }  
                  recover-time  
                  }`

**Hierarchy Level**    [edit system [ddos-protection](#)]

**Release Information**    Statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.

**Description**    Configure DDoS policers for all packet types within a protocol group.

**Options**    **aggregate**—Configure the policer that polices all control packets belonging to the specified protocol as a combined group. An aggregate policer exists for all protocol groups.

**protocol-group**—Name of the protocol group for which traffic is policed. You can configure the aggregate policer for any of the following protocol groups listed in [Table 16 on page 281](#). The table shows the default configuration for the policers.

Table 16: Protocol Groups Supported by DDoS Protection on QFX Series Switches

| Protocol Group          | Description                                          | Default Bandwidth | Default Burst |
|-------------------------|------------------------------------------------------|-------------------|---------------|
| <b>arp</b>              | ARP traffic                                          | 500               | 200           |
| <b>bfd</b>              | BFD and BFDv6                                        | 1200              | 200           |
| <b>bgp</b>              | BGP traffic                                          | 3000              | 200           |
| <b>bpdu</b>             | BPDU : LACP, STP, VSTP, LLDP                         | 1000              | 200           |
| <b>dhcpv4v6</b>         | DHCPv4 and DHCPv6                                    | 1000              | 200           |
| <b>fip-snooping</b>     | FIP snooping                                         | 1000              | 200           |
| <b>fw-host</b>          | Configure packets via firewall 'send-to-host' action | 500               | 10            |
| <b>garp-reply</b>       | Gratuitous ARP reply                                 | 100               | 10            |
| <b>igmp</b>             | IGMPv4 and IGMPv6 traffic                            | 1000              | 200           |
| <b>ip-opt</b>           | ?                                                    | 50                | 10            |
| <b>ipmcast-miss</b>     | IP multicast miss                                    | 1000              | 300           |
| <b>ipmc-reserved</b>    | IP multicast reserved                                | 1000              | 200           |
| <b>isis</b>             | IS-IS traffic                                        | 2000              | 200           |
| <b>l2pt</b>             | Layer 2 protocol tunneling traffic                   | 1000              | 200           |
| <b>l3-dest-miss</b>     | Layer 3 destination miss                             | 100               | 10            |
| <b>l3mc-sgv-hit-icl</b> | Layer 3 multicast (*, G) hit ICL                     | 100               | 10            |
| <b>l3-mtu-fail</b>      | Layer 3 MTU fail                                     | 50                | 10            |
| <b>l3nhop</b>           | Layer 3 next hop                                     | 300               | 200           |
| <b>lACP</b>             | LACP traffic                                         | 250               | 200           |
| <b>ldp</b>              | LDP traffic                                          | 3000              | 200           |
| <b>lldp</b>             | LLDP traffic                                         | 1000              | 200           |
| <b>localnh</b>          | Local next hop                                       | 1500              | 200           |
| <b>martian-address</b>  | Martian address                                      | 50                | 10            |

Table 16: Protocol Groups Supported by DDoS Protection on QFX Series Switches (*continued*)

| Protocol Group         | Description                                                                                             | Default Bandwidth | Default Burst |
|------------------------|---------------------------------------------------------------------------------------------------------|-------------------|---------------|
| <b>ndpv6</b>           | Neighbor Discovery Protocol traffic                                                                     | 500               | 200           |
| <b>nonucast-switch</b> | Non-unicast switched                                                                                    | 300               | 10            |
| <b>ntp</b>             | NTP traffic                                                                                             | 100               | 10            |
| <b>ospf</b>            | OSPF traffic                                                                                            | 3000              | 200           |
| <b>ospf-hello</b>      | OSPF hello packets                                                                                      | 1500              | 200           |
| <b>pim-ctrl</b>        | PIM control packets                                                                                     | 1500              | 200           |
| <b>pim-data</b>        | PIM data                                                                                                | 1500              | 200           |
| <b>pvstp</b>           | PVSTP traffic                                                                                           | 1000              | 200           |
| <b>redirect</b>        | ICMP redirect                                                                                           | 100               | 10            |
| <b>resolve</b>         | Unclassified IPv4 and IPv6 resolve packets sent to the host because of a traffic request resolve action | 300               | 200           |
| <b>rip</b>             | RIP traffic                                                                                             | 3000              | 200           |
| <b>rsvp</b>            | RSVP traffic                                                                                            | 3000              | 200           |
| <b>sample-dest</b>     | Sample destination                                                                                      | 2000              | 200           |
| <b>sample-source</b>   | Sample source                                                                                           | 2000              | 200           |
| <b>stp</b>             | STP traffic                                                                                             | 1000              | 200           |
| <b>tll</b>             | Time to Live packets                                                                                    | 50                | 10            |
| <b>unknown-l2mc</b>    | Unknown Layer 2 multicast                                                                               | 3000              | 200           |
| <b>urpf-fail</b>       | Unicast reverse-path forwarding failure                                                                 | 50                | 10            |
| <b>vchassis</b>        | Virtual Chassis                                                                                         | 500               | 200           |
| <b>vcipc</b>           | VC IPC                                                                                                  | 1000              | 200           |
| <b>vcudp</b>           | VC UDP packets                                                                                          | 1000              | 200           |
| <b>vxlan</b>           | VXLAN Layer 2 and Layer 3 packets                                                                       | 300               | 10            |

The remaining statements are explained separately.



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

**Related Documentation** • [Configuring DDoS Protection Policers on QFX Series Switches on page 174](#)

## recover-time (DDoS)

**Syntax** recover-time *seconds*;

**Hierarchy Level** [edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]

**Release Information** Statement introduced in Junos OS Release 11.2.  
Statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.

**Description** (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or QFX5100 switches) Configure how much time must pass since the last detected DDoS violation before the traffic is considered to have recovered from the attack and returned to normal.



**NOTE:** Packet-type policers are not supported on QFX5100 switches.

**Options** *seconds*—Period required for the traffic to recover.  
**Range:** 1 through 3600 seconds  
**Default:** 300

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

**Related Documentation** • [Configuring DDoS Protection Policers for Individual Packet Types](#)  
• [Configuring DDoS Protection Policers on QFX Series Switches on page 174](#)

## traceoptions (DDoS)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;         &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;     level (all   error   info   notice   verbose   warning);     no-remote-trace; } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>     | [edit system ddos-protection]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b> | <p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>         | Define tracing operations for DDoS protection processes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Options</b>             | <p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory <code>/var/log</code>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Trace all operations.</li> <li>• <b>config</b>—Trace processing of the DDoS configuration at an extensive level.</li> <li>• <b>events</b>—Trace jddosd event processing; currently only exit events are traced.</li> <li>• <b>gres</b>—Trace messages exchanged with the kernel and jddosd process that could affect.</li> <li>• <b>init</b>—Trace jddosd initialization.</li> <li>• <b>memory</b>—Trace memory management code. This flag is not currently supported.</li> <li>• <b>protocol</b>—Trace DDoS protocol state processing. Only the violation state is currently traced.</li> <li>• <b>rtsock</b>—Trace messages exchanged with the kernel and jddosd process.</li> <li>• <b>signal</b>—Trace system signals that are passed to jddosd, such as SIGTERM.</li> <li>• <b>state</b>—Trace state machine events. This flag is not currently supported.</li> <li>• <b>timer</b>—Trace jddosd timer events.</li> <li>• <b>ui</b>—Trace user interface processing. This flag is not currently supported.</li> </ul> <p><b>level</b>—Level of tracing to perform. You can specify any of the following levels:</p> |

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

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

**no-remote-trace**—Disable remote tracing.

**no-world-readable**—(Optional) Disable unrestricted file access.

**size *maximum-file-size***—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**Syntax:** *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

**Range:** 10,240 through 1,073,741,824

**world-readable**—(Optional) Enable unrestricted file access.

|                                 |                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Required Privilege Level</b> | <b>trace</b> —To view this statement in the configuration.                                    |
|                                 | <b>trace-control</b> —To add this statement to the configuration.                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Tracing DDoS Protection Operations</i></li> </ul> |



## CHAPTER 15

# Firewall Operational Commands

- `clear firewall`
- `show firewall`
- `show firewall policer`
- `show interfaces filters`
- `show pfe filter hw summary`

## clear firewall

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>clear firewall (all   counter <i>counter-name</i>   filter <i>filter-name</i>)</code>                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.1 for the QFX Series.<br>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                                                   |
| <b>Description</b>              | <p>Clear statistics provided by firewall filters.</p> <p>When you clear the counters of a filter, this not only impacts the counters shown by the CLI, but also the ones tracked by SNMP 2.</p>                                                                                                                                                                             |
| <b>Options</b>                  | <p><b>all</b>—Clear the packet and byte counts for all firewall filter counters and clear the packet counts for all policer counters.</p> <p><b>counter <i>counter-name</i></b>—Clear the packet and byte counts for the specified firewall filter counter.</p> <p><b>filter <i>filter-name</i></b>—Clear the packet and byte counts for the specified firewall filter.</p> |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Verifying That Firewall Filters Are Operational on page 50</a></li><li>• <a href="#">Verifying That Two-Color Policers Are Operational on page 85</a></li><li>• <a href="#">Overview of Firewall Filters on page 3</a></li><li>• <a href="#">Overview of Policers on page 61</a></li></ul>                              |

## Sample Output

### clear firewall all

```
user@switch> clear firewall all
```

### clear firewall counter

```
user@switch> clear firewall counter port-filter-counter
```

### clear firewall filter

```
user@switch> clear firewall filter ingress-port-filter
```

## show firewall

|                                 |                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show firewall<br><counter <i>counter-name</i> ><br><filter <i>filter-name</i> ><br><log <detail   interface <i>interface-name</i> >><br><terse>                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.1 for the QFX Series.<br>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                                                           |
| <b>Description</b>              | Display statistics about configured firewall filters.                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                  | <p><b>counter <i>counter-name</i></b>—(Optional) Display statistics about a particular firewall filter counter.</p> <p><b>filter <i>filter-name</i></b>—(Optional) Display statistics about a particular firewall filter.</p> <p><b>log</b>—(Optional) Display log entries for all firewall filter activity.</p> <p><b>terse</b>—(Optional) Display firewall filter names only.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Verifying That Firewall Filters Are Operational on page 50</a></li> <li>• <a href="#">Verifying That Two-Color Policers Are Operational on page 85</a></li> <li>• <a href="#">Overview of Firewall Filters on page 3</a></li> <li>• <a href="#">Overview of Policers on page 61</a></li> </ul>                                 |
| <b>List of Sample Output</b>    | <a href="#">show firewall on page 290</a><br><a href="#">show firewall filter <i>filter-name</i> on page 291</a><br><a href="#">show firewall counter <i>counter-name</i> on page 291</a><br><a href="#">show firewall log on page 291</a><br><a href="#">show firewall log detail on page 291</a>                                                                                  |
| <b>Output Fields</b>            | <a href="#">Table 17 on page 289</a> lists the output fields for the <b>show firewall</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                          |

**Table 17: show firewall Output Fields**

| Field Name | Field Description                                                                                                     | Level of Output |
|------------|-----------------------------------------------------------------------------------------------------------------------|-----------------|
| Filter     | Name of the filter that is configured at the <b>[edit firewall family <i>family-name</i> filter]</b> hierarchy level. | All levels      |

Table 17: show firewall Output Fields (*continued*)

| Field Name           | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                         | Level of Output |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Counters</b>      | Display filter counter information: <ul style="list-style-type: none"> <li>Name—Name of a filter counter that has been configured with the <b>count</b> firewall filter action modifier.</li> <li>Bytes—Number of bytes that match the filter term where the <b>count</b> action modifier was specified.</li> <li>Packets—Number of packets that matched the filter term where the <b>count</b> action modifier was specified.</li> </ul> | All levels      |
| <b>Policers</b>      | Display policer information: <ul style="list-style-type: none"> <li>Name—Name of the policer that is configured at the <b>[edit firewall policer]</b> hierarchy level.</li> <li>Packets—Number of packets that matched the filter term where the <b>policer</b> action modifier was specified. This is the number of packets that exceeded the rate limits that the policer specifies.</li> </ul>                                         | All levels      |
| <b>Action</b>        | Filter action: <ul style="list-style-type: none"> <li>A—Accept</li> <li>D—Discard</li> </ul>                                                                                                                                                                                                                                                                                                                                              | All levels      |
| <b>Interface</b>     | Interface on which the firewall filter is applied.                                                                                                                                                                                                                                                                                                                                                                                        | All levels      |
| <b>Protocol</b>      | Name of the packet protocol.                                                                                                                                                                                                                                                                                                                                                                                                              | All levels      |
| <b>Packet Length</b> | Length of the packet.                                                                                                                                                                                                                                                                                                                                                                                                                     | All levels      |
| <b>Src Addr</b>      | Source address of the packet.                                                                                                                                                                                                                                                                                                                                                                                                             | All levels      |
| <b>Dest Addr</b>     | Destination address of the packet.                                                                                                                                                                                                                                                                                                                                                                                                        | All levels      |

## Sample Output

### show firewall

```

user@switch> show firewall
Filter: egress-vlan-watch-employee
Counters:
Name Bytes Packets
counter-employee-web 0 0
Filter: ingress-port-limit-tcp-icmp
Counters:
Name Bytes Packets
icmp-counter 560 10
Policers:
Name Packets
icmp-connection-policer 10
tcp-connection-policer 0
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest

```



**show firewall filter filter-name**

```

user@switch> show firewall filter ingress-port-limit-tcp-icmp
Filter: ingress-port-limit-tcp-icmp
Counters:
Name Bytes Packets
icmp-counter 560 10
Policers:
Name Packets
icmp-connection-policer 10
tcp-connection-policer 0

```

**show firewall counter counter-name**

```

user@switch> show firewall counter icmp-counter
Filter: ingress-port-voip-class-filter
Counters:
Name Bytes Packets
icmp-counter 560 10

```

**show firewall log**

```

user@switch> show firewall log
Log :

Time Filter Action Interface Protocol Src Addr
 Dest Addr
08:00:53 pfe R ge-1/0/6.0 ICMP 192.168.3.5
 192.168.3.4
08:00:52 pfe R ge-1/0/6.0 ICMP 192.168.3.5
 192.168.3.4
08:00:51 pfe R ge-1/0/6.0 ICMP 192.168.3.5
 192.168.3.4
08:00:50 pfe R ge-1/0/6.0 ICMP 192.168.3.5
 192.168.3.4
08:00:49 pfe R ge-1/0/6.0 ICMP 192.168.3.5
 192.168.3.4
08:00:48 pfe R ge-1/0/6.0 ICMP 192.168.3.5
 192.168.3.4
08:00:47 pfe R ge-1/0/6.0 ICMP 192.168.3.5
 192.168.3.4

```

**show firewall log detail**

```

user@switch> show firewall log detail
Log :

Time of Log: 2010-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0Name of protocol: TCP, Packet Length: 50824, Source address:
172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2010-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 1020, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2010-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2010-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of

```

```
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2010-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2010-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
```

## show firewall policer

|                                 |                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show firewall policer</code><br><code>&lt;policer-name&gt;</code>                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.1 for the QFX Series.<br>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                                                                                                                                                                                           |
| <b>Description</b>              | Display statistics about configured policers.                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>                  | <b>none</b> —Display the count of policed packets for all configured policers.<br><br><b>policer-name</b> —(Optional) Display the count of policed packets for the specified policer.                                                                                                                                                               |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Verifying That Firewall Filters Are Operational on page 50</a></li> <li>• <a href="#">Verifying That Two-Color Policers Are Operational on page 85</a></li> <li>• <a href="#">Overview of Firewall Filters on page 3</a></li> <li>• <a href="#">Overview of Policers on page 61</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show firewall policer on page 293</a><br><a href="#">show firewall policer policer-name on page 294</a>                                                                                                                                                                                                                                 |
| <b>Output Fields</b>            | <a href="#">Table 18 on page 293</a> lists the output fields for the <b>show firewall policer</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                  |

Table 18: show firewall policer Output Fields

| Field Name      | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                 | Level of Output |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Filter</b>   | Name of the filter that is configured at the <code>[edit firewall family <i>family-name</i> filter]</code> hierarchy level.                                                                                                                                                                                                                                                                                                       | All levels      |
| <b>Policers</b> | Display policer information: <ul style="list-style-type: none"> <li>• <b>Filter</b>—Name of filter that specifies the <b>policer</b> action modifier.</li> <li>• <b>Name</b>—Name of policer.</li> <li>• <b>Packets</b>—Number of packets that matched the filter term in which the <b>policer</b> action modifier is specified. This is the number of packets that exceed the rate limits that the policer specifies.</li> </ul> | All levels      |

## Sample Output

### show firewall policer

```
user@switch> show firewall policer
Filter: egress-vlan-filter
Filter: ingress-port-filter
```

```
Policers:
Name Packets
icmp-connection-policer 0
tcp-connection-policer 0
Filter: ingress-vlan-rogue-block
```

#### **show firewall policer policer-name**

```
user@switch> show firewall policer tcp-connection-policer
Filter: ingress-port-filter
Policers:
Name Packets
tcp-connection-policer 0
```

## show interfaces filters

|                                 |                                                                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show interfaces filters</code><br><code>&lt;interface-name&gt;</code>                                                                                                          |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.1 for the QFX Series.<br>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.                                            |
| <b>Description</b>              | Display firewall filters that are configured on each interface in a switch.                                                                                                          |
| <b>Options</b>                  | <b>none</b> —Display firewall filter information about all interfaces.<br><br><b>interface-name</b> —(Optional) Display firewall filter information about a particular interface.    |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show firewall on page 289</a></li> </ul>                                                                                        |
| <b>List of Sample Output</b>    | <a href="#">show interfaces filters on page 295</a><br><a href="#">show interfaces filters interface-name on page 296</a>                                                            |
| <b>Output Fields</b>            | <a href="#">Table 19 on page 295</a> lists the output fields for the <b>show interfaces filters</b> command. Output fields are listed in the approximate order in which they appear. |

Table 19: show interfaces filters Output Fields

| Field Name           | Field Description                                                                          | Level of Output |
|----------------------|--------------------------------------------------------------------------------------------|-----------------|
| <b>Interface</b>     | Name of the physical interface.                                                            | All levels      |
| <b>Admin</b>         | Interface state: <b>up</b> or <b>down</b> .                                                | All levels      |
| <b>Link</b>          | Link state: <b>up</b> or <b>down</b> .                                                     | All levels      |
| <b>Proto</b>         | Protocol that is configured on the interface.                                              | All levels      |
| <b>Input Filter</b>  | Name of the firewall filter to be evaluated when packets are received on the interface.    | All levels      |
| <b>Output Filter</b> | Name of the firewall filter to be evaluated when packets are transmitted on the interface. | All levels      |

## Sample Output

### show interfaces filters

```

user@switch> show interfaces filters
Interface Admin Link Proto Input Filter Output Filter
ge-0/0/6 up up inet
ge-0/0/6.0 up up inet

```

|             |    |      |
|-------------|----|------|
| ge-0/0/7    | up | down |
| ge-0/0/8    | up | down |
| ge-0/0/9    | up | down |
| ge-0/0/10   | up | down |
| ge-0/0/10.0 | up | down |

**show interfaces filters interface-name**

```
user@switch> show interfaces filters ge-0/0/6
```

| Interface  | Admin | Link | Proto | Input Filter | Output Filter |
|------------|-------|------|-------|--------------|---------------|
| ge-0/0/6   | up    | up   |       |              |               |
| ge-0/0/6.0 | up    | up   | inet  |              |               |

## show pfe filter hw summary

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show pfe filter hw summary                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Command introduced in Junos OS Release 14.1X53-D10 for the QFX Series.                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>              | <p>Display a summary of the access control list (ACL; also known as firewall filter) ternary content-addressable memory (TCAM) hardware utilization to show the allocated, used, and free TCAM entry space.</p> <p>Command supported on standalone QFX Series switches, QFX5100-only (pure QFX5100) Virtual Chassis Fabric (VCF), QFX5100-only (pure QFX5100) Virtual Chassis (VC), and QFX3500-only (pure QFX3500) VC.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Planning the Number of Firewall Filters to Create on page 34</a></li> </ul>                                                                                                                                                                                                                                                                                            |
| <b>List of Sample Output</b>    | <a href="#">show pfe filter hw summary on page 298</a>                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Output Fields</b>            | <p><a href="#">Table 20 on page 297</a> lists the output fields for the <b>show pfe filter hw summary</b> command. Output fields are listed in the approximate order in which they appear.</p>                                                                                                                                                                                                                              |

**Table 20: show pfe filter hw summary Output Fields**

| Field Name       | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Group</b>     | <p>ACL ingress and egress filter groups:</p> <ul style="list-style-type: none"> <li>• iRACL group—ingress routing ACL filter group</li> <li>• iVACL group—ingress VLAN ACL filter group</li> <li>• iPACL group—ingress port ACL filter group</li> <li>• ePACL group—egress port ACL filter group</li> <li>• eVACL group—egress VLAN ACL filter group</li> <li>• eRACL group—egress routing ACL filter group</li> <li>• eRACL IPv6 group—egress IPv6 routing ACL filter group</li> </ul> |
| <b>Group-ID</b>  | Internal identification number of the filter group.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Allocated</b> | Number of TCAM filter entries allocated to the filter group.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Used</b>      | Number of TCAM filter entries used by the filter group.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Free</b>      | Number of TCAM filter entries available for use by the filter group.                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Sample Output

### show pfe filter hw summary

```
user@switch> show pfe filter hw summary
```

| Group                    | Group-ID | Allocated | Used | Free |
|--------------------------|----------|-----------|------|------|
| -----                    |          |           |      |      |
| > Ingress filter groups: |          |           |      |      |
| iRACL group              | 14       | 512       | 4    | 508  |
| iVACL group              | 13       | 512       | 2    | 510  |
| iPACL group              | 12       | 256       | 2    | 254  |
| > Egress filter groups:  |          |           |      |      |
| ePACL group              | 20       | 256       | 3    | 253  |
| eVACL group              | 21       | 256       | 4    | 252  |
| eRACL group              | 22       | 256       | 245  | 11   |
| eRACL IPV6 group         | 24       | 256       | 3    | 253  |



## CHAPTER 16

# MACsec Operational Commands

- clear security mka statistics
- show security macsec connections
- show security macsec statistics
- show security mka sessions
- show security mka statistics

## clear security mka statistics

---

|                                 |                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear security mka statistics<br><interface <i>interface-name</i> >                                                                                                                                                                                                   |
| <b>Release Information</b>      | Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Command introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                                             |
| <b>Description</b>              | <p>Clear—reset to zero (0)—all MACsec Key Agreement (MKA) protocol statistics.</p> <p>You are clearing the statistics that are viewed using the <b>show security mka statistics</b> when you enter this command.</p>                                                  |
| <b>Options</b>                  | <p><b>none</b>—Clear all MKA counters for all interfaces on the switch.</p> <p><b>interface <i>interface-name</i></b>—(Optional) Clear MKA traffic counters for the specified interface only.</p>                                                                     |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                 |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">show security mka statistics on page 309</a></li><li>• <a href="#">show security mka sessions on page 307</a></li><li>• <a href="#">Understanding Media Access Control Security (MACsec) on page 93</a></li></ul> |

## Sample Output

### clear security mka statistics

```
user@switch> clear security mka statistics
```

## show security macsec connections

|                                 |                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show security macsec connections<br><interface <i>interface-name</i> >                                                                                                                                                 |
| <b>Release Information</b>      | Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Command introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                              |
| <b>Description</b>              | Display the status of the active MACsec connections on the switch.                                                                                                                                                     |
| <b>Options</b>                  | <b>none</b> —Display MACsec connection information for all interfaces on the switch.<br><br><b>interface <i>interface-name</i></b> —(Optional) Display MACsec connection information for the specified interface only. |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">show security macsec statistics on page 303</a></li> </ul>                                                                                                        |
| <b>List of Sample Output</b>    | <a href="#">show security macsec connections on page 302</a>                                                                                                                                                           |
| <b>Output Fields</b>            | <a href="#">Table 21 on page 301</a> lists the output fields for the <b>show security macsec connections</b> command. Output fields are listed in the approximate order in which they appear.                          |

Table 21: show security macsec connections Output Fields

| Field Name           | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fields for Interface |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Interface name       | Name of the interface.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| CA name              | Name of the connectivity association.<br><br>A connectivity association is named using the <b>connectivity-association</b> statement when you are enabling MACsec.                                                                                                                                                                                                                                                                                     |
| Cipher suite         | Name of the cipher suite used for encryption.                                                                                                                                                                                                                                                                                                                                                                                                          |
| Encryption           | Encryption setting. Encryption is enabled when this output is <b>on</b> and disabled when this output is <b>off</b> .<br><br>The encryption setting is set using the <b>no-encryption</b> statement in the connectivity association when using static connectivity association key (CAK) security mode and is set using the <b>encryption</b> statement in the secure channel when using static secure association key (SAK) or dynamic security mode. |
| Key server offset    | Offset setting.<br><br>The offset is set using the <b>offset</b> statement when configuring the connectivity association when using static connectivity association key (CAK) or dynamic security mode or the secure channel when using static secure association key (SAK) security mode.                                                                                                                                                             |

Table 21: show security macsec connections Output Fields (*continued*)

| Field Name            | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Include SCI</b>    | <p>SCI tagging. The SCI tag is included on packets in a secure channel when this output is <b>yes</b>, and not included on packets in a secure channel when this output is <b>no</b>.</p> <p>You can enable SCI tagging using the <b>include-sci</b> statement in the connectivity association.</p> <p><b>NOTE:</b> SCI tags are automatically appended to packets leaving a MACsec-enabled interface on an EX4300 switch. The <b>include-sci</b> option is, therefore, not available on EX4300 switches. The output for the <b>Include SCI</b> field is <b>yes</b>.</p> |
| <b>Replay protect</b> | <p>Replay protection setting. Replay protection is enabled when this output is <b>on</b> and disabled when this output is <b>off</b>.</p> <p>You can enable replay protection using the <b>replay-protect</b> statement in the connectivity association.</p>                                                                                                                                                                                                                                                                                                             |
| <b>Replay window</b>  | <p>Replay protection window setting. This output is set to <b>0</b> when replay protection is disabled, and is the size of the replay window, in number of packets, when replay protection is enabled.</p> <p>The size of the replay window is configured using the <b>replay-window-size</b> statement in the connectivity association.</p>                                                                                                                                                                                                                             |

## Sample Output

### show security macsec connections

```

user@host> show security macsec connections
Interface name: xe-0/1/0
 CA name: CA1
 Cipher suite: GCM-AES-128 Encryption: on
 Key server offset: 0 Include SCI: no
 Replay protect: off Replay window: 0

```

show security macsec statistics

Syntax

show security macsec statistics  
<brief | detail>  
<interface *interface-name*>

Release Information

Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.  
Command introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.

Description

Display Media Access Control Security (MACsec) statistics.


Options

none

—Display MACsec statistics in brief form for all interfaces on the switch.

brief | detail

—(Optional) Display the specified level of output. Using the **brief** option is equivalent to entering the command with no options (the default). The **detail** option displays additional fields that are not visible in the **brief** output.



NOTE:

The field names that only appear in this command output when you enter the **detail** option are mostly useful for debugging purposes by Juniper Networks support personnel.

interface *interface-name*

—(Optional) Display MACsec statistics for the specified interface only.

Required Privilege Level

view

Related Documentation

- [show security macsec connections on page 301](#)

List of Sample Output

[show security macsec statistics interface xe-0/1/0 detail on page 305](#)

Output Fields

Table 22 on page 303 lists the output fields for the **show security macsec statistics** command. Output fields are listed in the approximate order in which they appear.

The field names that appear in this command output only when you enter the **detail** option are mostly useful for debugging purposes by Juniper Networks support personnel. Those field names are, therefore, not included in this table.

Table 22: show security macsec statistics Output Fields

| Field Name                            | Field Description      | Level of Output |
|---------------------------------------|------------------------|-----------------|
| Interface name                        | Name of the interface. | All levels      |
| Fields for Secure Channel transmitted |                        |                 |

Table 22: show security macsec statistics Output Fields (*continued*)

| Field Name                                       | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                 | Level of Output |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Encrypted packets</b>                         | <p>Total number of packets transmitted out of the interface in the secure channel that were secured and encrypted using MACsec.</p> <p>Data packets are sent in the secure channel when MACsec is enabled, and are secured using a secure association key (SAK).</p>                                                                                                                                                              | All levels      |
| <b>Encrypted bytes</b>                           | <p>Total number of bytes transmitted out of the interface in the secure channel that were secured and encrypted using MACsec.</p> <p>Data packets are sent in the secure channel when MACsec is enabled, and are secured using a secure association key (SAK).</p>                                                                                                                                                                | All levels      |
| <b>Protected packets</b>                         | <p>Total number of packets transmitted out of the interface in the secure channel that were secured but not encrypted using MACsec.</p> <p>Data packets are sent in the secure channel when MACsec is enabled, and are secured using a secure association key (SAK).</p>                                                                                                                                                          | All levels      |
| <b>Protected bytes</b>                           | <p>Total number of bytes transmitted out of the interface in the secure channel that were secured but not encrypted using MACsec.</p> <p>Data packets are sent in the secure channel when MACsec is enabled, and are secured using a secure association key (SAK).</p>                                                                                                                                                            | All levels      |
| <b>Fields for Secure Association transmitted</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                   |                 |
| <b>Encrypted packets</b>                         | <p>Total number of packets transmitted out of the interface in the connectivity association that were secured and encrypted using MACsec.</p> <p>The total includes the data packets transmitted in the secure channel and secured using a SAK and the control packets secured using a connectivity association key (CAK).</p>                                                                                                    | All levels      |
| <b>Protected packets</b>                         | <p>Total number of packets transmitted out of the interface in the connectivity association that were secured but not encrypted using MACsec.</p> <p>The total includes the data packets transmitted in the secure channel and secured using a SAK and the control packets secured using a connectivity association key (CAK).</p>                                                                                                | All levels      |
| <b>Fields for Secure Channel received</b>        |                                                                                                                                                                                                                                                                                                                                                                                                                                   |                 |
| <b>Accepted packets</b>                          | <p>The number of received packets that have been accepted by the secure channel on the interface. The secure channel is used to send all data plane traffic on a MACsec-enabled link.</p> <p>A packet is considered accepted for this counter when it has been received by this interface and it has passed the MACsec integrity check.</p> <p>This counter increments for traffic that is and is not encrypted using MACsec.</p> | All levels      |

Table 22: show security macsec statistics Output Fields (*continued*)

| Field Name                                    | Field Description                                                                                                                                                                                                                                                                                                                                                                                     | Level of Output |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Validated bytes</b>                        | <p>The number of bytes that have been validated by the MACsec integrity check and received on the secure channel on the interface. The secure channel is used to send all data plane traffic on a MACsec-enabled link.</p> <p>This counter does not increment when MACsec encryption is disabled.</p>                                                                                                 | All levels      |
| <b>Decrypted bytes</b>                        | <p>The number of bytes received in the secure channel on the interface that have been decrypted. The secure channel is used to send all data plane traffic on a MACsec-enabled link.</p> <p>An encrypted byte has to be decrypted before it can be received on the receiving interface. The decrypted bytes counter is incremented for received traffic that was encrypted using MACsec.</p>          | All levels      |
| <b>Fields for Secure Association received</b> |                                                                                                                                                                                                                                                                                                                                                                                                       |                 |
| <b>Accepted packets</b>                       | <p>The number of received packets that have been accepted in the connectivity association on the interface. The counter includes all control and data plane traffic accepted on the interface.</p> <p>A packet is considered accepted for this counter when it has been received by this interface and it has passed the MACsec integrity check.</p>                                                  | All levels      |
| <b>Validated bytes</b>                        | <p>The number of bytes that have been validated by the MACsec integrity check and received on the connectivity association on the interface. The counter includes all control and data plane traffic accepted on the interface.</p> <p>This counter does not increment when MACsec encryption is disabled.</p>                                                                                        | All levels      |
| <b>Decrypted bytes</b>                        | <p>The number of bytes received in the connectivity association on the interface that have been decrypted. The counter includes all control and data plane traffic accepted on the interface.</p> <p>An encrypted byte has to be decrypted before it can be received on the receiving interface. The decrypted bytes counter is incremented for received traffic that was encrypted using MACsec.</p> | All levels      |

## Sample Output

### show security macsec statistics interface xe-0/1/0 detail

```
user@host> show security macsec statistics interface xe-0/1/0 detail
```

```
Interface name: xe-0/1/0
Secure Channel transmitted
 Encrypted packets: 123858
 Encrypted bytes: 32190903
 Protected packets: 0
 Protected bytes: 0
Secure Association transmitted
```

```
 Encrypted packets: 123858
 Protected packets: 0
Secure Channel received
 Accepted packets: 123877
 Validated bytes: 0
 Decrypted bytes: 32196238
Secure Association received
 Accepted packets: 123877
 Validated bytes: 0
 Decrypted bytes: 32196238
Error and debug
Secure Channel transmitted packets
 Untagged: 0, Too long: 0
Secure Channel received packets
 Control: 0, Tagged miss: 3202804
 Untagged hit: 0, Untagged: 0
 No tag: 0, Bad tag: 0
 Unknown SCI: 0, No SCI: 0
 Control pass: 0, Control drop: 0
 Uncontrol pass: 123877, Uncontrol drop: 0
 Hit dropped: 0, Invalid accept: 0
 Late drop: 0, Delayed accept: 0
 Unchecked: 0, Not valid drop: 0
 Not using SA drop: 0, Unused SA accept: 0
```



## show security mka sessions

|                                 |                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show security mka sessions<br><interface <i>interface-name</i> >                                                                                                                                                                                      |
| <b>Release Information</b>      | Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Command introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                             |
| <b>Description</b>              | Display MACsec Key Agreement (MKA) session information.                                                                                                                                                                                               |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li><b>interface <i>interface-name</i></b>—(Optional) Display the MKA session information for the specified interface only.</li> </ul>                                                                             |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">show security mka statistics on page 309</a></li> <li><a href="#">show security macsec connections on page 301</a></li> <li><a href="#">show security macsec statistics on page 303</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show security mka sessions on page 308</a>                                                                                                                                                                                                |
| <b>Output Fields</b>            | Table 23 on page 307 lists the output fields for the <b>show security mka sessions</b> command. Output fields are listed in the approximate order in which they appear.                                                                               |

Table 23: show security mka sessions Output Fields

| Field Name        | Field Description                                                                                                                                    |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface name    | Name of the interface.                                                                                                                               |
| Member identifier | Name of the member identifier.                                                                                                                       |
| CAK name          | Name of the Connectivity Association Key (CAK).<br>The CAK is configured using the <b>cak</b> keyword when configuring the pre-shared key.           |
| Transmit interval | The transmit interval.                                                                                                                               |
| Outbound SCI      | Name of the outbound secure channel identifier.                                                                                                      |
| Message number    | Number of the last data message.                                                                                                                     |
| Key number        | Key number.                                                                                                                                          |
| Key server        | Key server status.<br>The switch is the key server when this output is <b>yes</b> . The switch is not the key server when this output is <b>no</b> . |

Table 23: show security mka sessions Output Fields (*continued*)

| Field Name           | Field Description                                                                                                  |
|----------------------|--------------------------------------------------------------------------------------------------------------------|
| Key server priority  | The key server priority.<br><br>The key server priority can be set using the <b>key-server-priority</b> statement. |
| Latest SAK AN        | Name of the latest secure association key (SAK) association number.                                                |
| Latest SAK KI        | Name of the latest secure association key (SAK) key identifier.                                                    |
| Fields for Peer list |                                                                                                                    |
| Member identifier    | Name of the member identifier.                                                                                     |
| Hold time            | Hold time, in seconds.                                                                                             |
| Message number       | Number of the last data message                                                                                    |
| SCI                  | Name of the secure channel identifier.                                                                             |
| Lowest acceptable PN | Number of the lowest acceptable packet number (PN).                                                                |

## Sample Output

### show security mka sessions

```
user@host> show security mka sessions
```

```
Interface name: xe-0/1/0
Member identifier: 0CCBEE42F8778300F8D0C1DC
CAK name: 1234567890
Transmit interval: 2000(ms)
Outbound SCI: 2C:6B:F5:9D:4B:1B/1
Message number: 1526465 Key number: 0
Key server: no Key server priority: 15
Latest SAK AN: 0 Latest SAK KI: 4F18CE25228178FD15976E4C/1
Previous SAK AN: 0 Previous SAK KI: 000000000000000000000000/0
Peer list
1. Member identifier: 4F18CE25228178FD15976E4C (live)
 Message number: 1526484 Hold time: 14500 (ms)
 SCI: 2C:6B:F5:9D:3A:1B/1
 Lowest acceptable PN: 121198
```

## show security mka statistics

|                                 |                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | show security mka statistics<br><interface <i>interface-name</i> >                                                                                                                                                                                  |
| <b>Release Information</b>      | Command introduced in Junos OS Release 13.2X50-D15 for EX Series switches.<br>Command introduced in Junos OS Release 14.1X53-D15 for QFX Series switches.                                                                                           |
| <b>Description</b>              | Display MACsec Key Agreement (MKA) protocol statistics.<br><br>The output for this command does not include statistics for MACsec data traffic. For MACsec data traffic statistics, see <a href="#">show security macsec statistics</a> .           |
| <b>Options</b>                  | <ul style="list-style-type: none"> <li><b>interface <i>interface-name</i></b>—(Optional) Display the MKA information for the specified interface only.</li> </ul>                                                                                   |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">show security mka sessions on page 307</a></li> <li><a href="#">show security macsec statistics on page 303</a></li> <li><a href="#">show security macsec connections on page 301</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show security mka statistics on page 310</a>                                                                                                                                                                                            |
| <b>Output Fields</b>            | <a href="#">Table 24 on page 309</a> lists the output fields for the <b>show security mka statistics</b> command. Output fields are listed in the approximate order in which they appear.                                                           |

**Table 24: show security mka statistics Output Fields**

| Field Name                      | Field Description                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Received packets</b>         | <p>Number of received MKA control packets.</p> <p>This counter increments for received MKA control packets only. This counter does not increment when data packets are received.</p>                                                                                                                        |
| <b>Transmitted packets</b>      | <p>Number of transmitted MKA packets</p> <p>This counter increments for transmitted MKA control packets only. This counter does not increment when data packets are transmitted.</p>                                                                                                                        |
| <b>Version mismatch packets</b> | Number of version mismatch packets.                                                                                                                                                                                                                                                                         |
| <b>CAK mismatch packets</b>     | <p>Number of Connectivity Association Key (CAK) mismatch packets.</p> <p>This counter increments when the connectivity association key (CAK) and connectivity association key name (CKN), which are user-configured values that have to match to enable MACsec, do not match for an MKA control packet.</p> |

Table 24: show security mka statistics Output Fields (*continued*)

| Field Name                           | Field Description                                                                                                                                                                 |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICV mismatch packets                 | Number of ICV mismatched packets.<br><br>This counter increments when the connectivity association key (CAK) value does not match on both ends of a MACsec-secured Ethernet link. |
| Duplicate message identifier packets | Number of duplicate message identifier packets.                                                                                                                                   |
| Duplicate message number packets     | Number of duplicate message number packets.                                                                                                                                       |
| Duplicate address packets            | Number of duplicate source MAC address packets.                                                                                                                                   |
| Invalid destination address packets  | Number of invalid destination MAC address packets.                                                                                                                                |
| Formatting error packets             | Number of formatting error packets.                                                                                                                                               |
| Old Replayed message number packets  | Number of old replayed message number packets.                                                                                                                                    |

## Sample Output

### show security mka statistics

```
user@host> show security mka statistics
```

```

Received packets: 1525844
Transmitted packets: 1525841
Version mismatch packets: 0
CAK mismatch packets: 0
ICV mismatch packets: 0
Duplicate message identifier packets: 0
Duplicate message number packets: 0
Duplicate address packets: 0
Invalid destination address packets: 0
Formatting error packets: 0
Old Replayed message number packets: 0
```

## CHAPTER 17

# Port Security Operational Commands

- clear arp inspection statistics
- clear dhcp snooping binding
- clear ethernet-switching port-error
- show dhcp snooping binding

## clear arp inspection statistics

---

|                                 |                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear arp inspection statistics<br><interface <i>interface</i> >                                                                                                                                                                         |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 12.1 for the QFX Series.                                                                                                    |
| <b>Description</b>              | Clear ARP inspection statistics.                                                                                                                                                                                                         |
| <b>Options</b>                  | <b>none</b> —Clears ARP statistics on all interfaces.<br><br><b>interface <i>interface-names</i></b> —(Optional) Clear ARP statistics on one or more interfaces.                                                                         |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>show arp inspection statistics</i></li><li>• <i>Example: Configuring Basic Port Security Features</i></li><li>• <a href="#">Verifying That DAI Is Working Correctly on page 135</a></li></ul> |
| <b>List of Sample Output</b>    | <a href="#">clear arp inspection statistics on page 312</a>                                                                                                                                                                              |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                         |

## Sample Output

### clear arp inspection statistics

```
user@switch> clear arp inspection statistics
```

## clear dhcp snooping binding

---

|                                 |                                                                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear dhcp snooping binding<br><mac (all   <i>mac-address</i> )><br><vlan (all   <i>vlan-name</i> )><br><vlan (all   <i>vlan-name</i> ) mac (all   <i>mac-address</i> )>                                                                                                |
| <b>Release Information</b>      | Command introduced in Junos OS Release 12.1 for the QFX Series.                                                                                                                                                                                                         |
| <b>Description</b>              | Clear the DHCP snooping database information.                                                                                                                                                                                                                           |
| <b>Options</b>                  | <p><b>mac (all   <i>mac-address</i>)</b>—(Optional) Clear DHCP snooping information for the specified MAC address or all MAC addresses.</p> <p><b>vlan (all   <i>vlan-name</i>)</b>—(Optional) Clear DHCP snooping information for the specified VLAN or all VLANs.</p> |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>Example: Configuring Basic Port Security Features</i></li> <li>• <a href="#">show dhcp snooping binding on page 315</a></li> </ul>                                                                                          |
| <b>List of Sample Output</b>    | <a href="#">clear dhcp snooping binding on page 313</a>                                                                                                                                                                                                                 |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                                                        |

## Sample Output

### clear dhcp snooping binding

```
user@switch> clear dhcp snooping binding
```

## clear ethernet-switching port-error

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | clear ethernet-switching port-error<br><interface <i>interface-name</i> >                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.1 for the QFX Series.                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>              | Clear all MAC limiting, MAC move limiting, and storm control errors from all the Ethernet switching interfaces on the switch or from the specified interface, and restore the interfaces or the specified interface to service.                                                                                                                                                            |
| <b>Options</b>                  | <b>none</b> —Clear all MAC limiting, MAC move limiting, and storm control errors from all the Ethernet switching interfaces on the switch and restore the interfaces to service.<br><br><b>interface <i>interface-name</i></b> —(Optional) Clear all MAC limiting, MAC move limiting, and storm control errors from the specified interface and restore the interface to service.          |
| <b>Required Privilege Level</b> | clear                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <i>Configuring MAC Limiting</i></li><li>• <i>Example: Configuring Storm Control to Prevent Network Outages</i></li><li>• <i>Configuring Port Security (CLI Procedure)</i></li><li>• <a href="#">port-error-disable on page 252</a></li><li>• <i>Configuring Autorecovery for MAC Limited or Storm Control Interfaces (CLI Procedure)</i></li></ul> |
| <b>Output Fields</b>            | This command produces no output.                                                                                                                                                                                                                                                                                                                                                           |



## show dhcp snooping binding

|                                 |                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show dhcp snooping binding</b><br><b>&lt;interface <i>interface-name</i>&gt;</b><br><b>&lt;vlan <i>vlan-name</i>&gt;</b>                                                                                                                         |
| <b>Release Information</b>      | Command introduced in Junos OS Release 9.0 for EX Series switches.<br>Command introduced in Junos OS Release 12.1 for the QFX Series.                                                                                                               |
| <b>Description</b>              | Display the DHCP snooping database information.                                                                                                                                                                                                     |
| <b>Options</b>                  | <b>interface <i>interface-name</i></b> —(Optional) Display the DHCP snooping database information for an interface.<br><br><b>vlan <i>vlan-name</i></b> —(Optional) Display the DHCP snooping database information for a VLAN.                      |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <i>clear dhcp snooping binding</i></li> <li>• <i>Example: Configuring Basic Port Security Features</i></li> <li>• <a href="#">Verifying That DHCP Snooping Is Working Correctly on page 131</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show dhcp snooping binding on page 315</a>                                                                                                                                                                                              |
| <b>Output Fields</b>            | <a href="#">Table 25 on page 315</a> lists the output fields for the <b>show dhcp snooping binding</b> command. Output fields are listed in the approximate order in which they appear.                                                             |

**Table 25: show dhcp snooping binding Output Fields**

| Field Name  | Field Description                                           | Level of Output |
|-------------|-------------------------------------------------------------|-----------------|
| MAC Address | MAC address of the network device; bound to the IP address. | All levels      |
| IP Address  | IP address of the network device; bound to the MAC address. | All levels      |
| Lease       | Lease granted to the IP address.                            | All levels      |
| Type        | How the MAC address was acquired.                           | All levels      |
| VLAN        | VLAN name of the network device whose MAC address is shown. | All levels      |
| Interface   | Interface address (port).                                   | All levels      |

## Sample Output

### show dhcp snooping binding

```
user@switch> show dhcp snooping binding
```

## DHCP Snooping Information:


| MAC Address       | IP Address | Lease | Type    | VLAN  | Interface   |
|-------------------|------------|-------|---------|-------|-------------|
| 00:00:01:00:00:03 | 192.0.2.0  | 640   | dynamic | guest | ge-0/0/12.0 |
| 00:00:01:00:00:04 | 192.0.2.1  | 720   | dynamic | guest | ge-0/0/12.0 |
| 00:00:01:00:00:05 | 192.0.2.5  | 800   | dynamic | guest | ge-0/0/13.0 |

## CHAPTER 18

# DDos Protection Operational Commands

- `clear ddos-protection protocols`
- `show ddos-protection protocols`
- `show ddos-protection protocols parameters`
- `show ddos-protection protocols statistics`
- `show ddos-protection statistics`
- `show ddos-protection version`

## clear ddos-protection protocols

|                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                           | <b>clear ddos-protection protocols</b><br><b>&lt;protocol-group &lt;packet-type&gt;&gt; (culprit-flows   states   statistics)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Release Information</b>                                                                                                                                              | Command introduced in Junos OS Release 11.2.<br>Option <b>culprit-flows</b> introduced in Junos OS Release 12.3.<br>Command introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>                                                                                                                                                      | Clear current DDoS protection statistics, violation states, or culprit flows for all packet types in all protocol groups, for all packet types in a particular protocol group, or for a particular packet type in a particular protocol group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <div>  <b>NOTE:</b> Packet-type policers are not supported on QFX5100 switches. </div> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                                                                                                                                                          | <p><b>protocol-group</b>—(Optional) Protocol group that is cleared. See <a href="#">show ddos-protection protocols</a> for a list of available groups on platforms other than QFX5100. See <a href="#">protocols</a> for a list of available groups on QFX5100.</p> <p><b>packet-type</b>—(Not available on QFX5100) (Optional) Packet type in a particular protocol group that is cleared. See <a href="#">show ddos-protection protocols</a> for a list of available packet types.</p> <p><b>culprit-flows</b>—Clear culprit flows for a packet type, for a protocol group, or for all protocol groups.</p> <p><b>states</b>—Clear DDoS protection violation states for a packet type, for a protocol group, or for all protocol groups.</p> <p><b>statistics</b>—Clear DDoS protection statistics such as packet counts and rates for a packet type, for a protocol group, or for all protocol groups.</p> |
| <b>Required Privilege Level</b>                                                                                                                                         | clear                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Related Documentation</b>                                                                                                                                            | <ul style="list-style-type: none"> <li>• <a href="#">show ddos-protection protocols on page 320</a></li> <li>• <a href="#">show ddos-protection statistics on page 354</a></li> <li>• <a href="#">show ddos-protection version on page 355</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>List of Sample Output</b>                                                                                                                                            | <a href="#">clear ddos-protection protocols on page 319</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Output Fields</b>                                                                                                                                                    | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Sample Output

`clear ddos-protection protocols`

```
user@host> clear ddos-protection protocols dhcpv4 bootp states
```

## show ddos-protection protocols

**Syntax** `show ddos-protection protocols <protocol-group (aggregate | packet-type)>`

**Release Information** Command introduced in Junos OS Release 11.2.  
Command introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.

**Description** Display DDoS protection configuration and statistics for protocol groups or individual packet types.



**NOTE:** Packet-type policers are not supported on QFX5100 switches.

**Options** **none**—Display information for all packet types in all protocol groups.

**aggregate**—(Optional) Display DDoS protection information for the aggregate policer.  
The **aggregate** option is available for all protocol groups.

**packet-type**—(Not available on QFX5100) (Optional) Display DDoS protection information for the specified packet type in the protocol group. The available packet types vary by protocol group. Only an aggregate policer is available for protocol groups that are not in the following list:

- **dhcpv4**—The following packet types are available for DHCPv4 traffic:
  - **ack**—DHCPACK packets.
  - **bad-packets**—DHCPv4 packets with bad formats.
  - **bootp**—DHCPBOOTP packets.
  - **decline**—DHCPDECLINE packets.
  - **discover**—DHCDISCOVER packets.
  - **force-renew**—DHCPFORCERENEW packets.
  - **inform**—DHCPINFORM packets.
  - **lease-active**—DHCPLEASEACTIVE packets.
  - **lease-query**—DHCPLEASEQUERY packets.
  - **lease-unassigned**—DHCPLEASEUNASSIGNED packets.
  - **lease-unknown**—DHCPLEASEUNKNOWN packets.
  - **nak**—DHCPNAK packets.
  - **no-message-type**—DHCP packets that are missing the message type..
  - **offer**—DHCOFFER packets.
  - **release**—DHCPACK packets.
  - **renew**—DHCPRENEW packets.

- **request**—DHCPREQUEST packets.
- **unclassified**— All unclassified packets in the protocol group.
- **dhcpv6**—The following packet types are available for DHCPv6 traffic:
  - **advertise**—ADVERTISE packets.
  - **confirm**—CONFIRM packets.
  - **decline**—DECLINE packets.
  - **information-request**—INFORMATION-REQUEST packets.
  - **leasequery**—LEASEQUERY packets.
  - **leasequery-data**—LEASEQUERY-DATA packets.
  - **leasequery-done**—LEASEQUERY-DONE packets.
  - **leasequery-reply**—LEASEQUERY-REPLY packets.
  - **rebind**—REBIND packets.
  - **reconfigure**—RECONFIGURE packets.
  - **relay-forward**—RELAY-FORWARD packets.
  - **relay-reply**—RELAY-REPLY packets.
  - **release**—RELEASE packets.
  - **renew**—RENEW packets.
  - **reply**—REPLY packets.
  - **request**—REQUEST packets.
  - **solicit**—SOLICIT packets.
  - **unclassified**— All unclassified packets in the protocol group.
- **filter-action**—The following packet types are available for unclassified firewall filter action packets, sent to the host because of reject terms in firewall filters:
  - **filter-v4**—Unclassified IPv4 filter action packets.
  - **filter-v6**—Unclassified IPv6 filter action packets.
  - **other**—All other unclassified filter action packets that are not IPv4 or IPv6.
- **frame-relay**—The following packet types are available for Frame Relay traffic:
  - **frf15**—Multilink frame relay FRF.15 packets.
  - **frf16**—Multilink frame relay FRF.16 packets.
- **ip-fragments**—The following packet types are available for IP fragments:
  - **first-fragment**—First IP fragment.
  - **trail-fragment**—Last IP fragment.

- **ip-options**—The following packet types are available for IP option traffic:
  - **non-v4v6**—Options packets other than IPv4/v6.
  - **router-alert**—Router alert options packets.
  - **unclassified**— All unclassified packets in the protocol group.
- **mcast-snoop**—Control traffic for multicast snooping.
  - **igmp**—Snooped IGMP traffic.
  - **pim**—Snooped PIM control traffic.
- **mlp**—The following MLP packet types are available:
  - **aging-exception**—MLP aging exception packets.
  - **packets**—MLP packets.
  - **unclassified**— All unclassified packets in the protocol group.
- **ppp**—The following PPP packet types are available:
  - **authentication**—PPP authentication protocol packets.
  - **echo-rep**—LCP echo reply packets.
  - **echo-req**—LCP echo request packets.
  - **ipcp**—IP Control Protocol packets.
  - **ipv6cp**—IPv6 Control Protocol packets.
  - **isis**—IS-IS packets.
  - **lcp**—Link Control Protocol packets.
  - **mlppp-lcp**—MLPPP LCP packets.
  - **mplscp**—MPLS Control Protocol packets.
  - **unclassified**— All unclassified packets in the protocol group.
- **pppoe**—The following PPPoE packet types are available:
  - **padi**—PADI packets.
  - **padm**—PADM packets.
  - **padn**—PADN packets.
  - **pado**—PADO packets.
  - **padr**—PADR packets.
  - **pads**—PADS packets.
  - **padt**—PADT packets.
- **radius**—The following RADIUS packet types are available:



- **accounting**—RADIUS accounting packets.
- **authorization**—RADIUS authorization packets.
- **server**—RADIUS server traffic.
- **unclassified**— All unclassified packets in the protocol group.
- **resolve**—The following packet types are available for unclassified resolve packets, which are sent to the host because of a traffic request resolve action:
  - **mcast-v4**—Unclassified IPv4 multicast resolve packets.
  - **mcast-v6**—Unclassified IPv6 multicast resolve packets.
  - **ucast-v4**—Unclassified IPv4 unicast resolve packets.
  - **ucast-v6**—Unclassified IPv6 unicast resolve packets.
  - **other**—All other unclassified resolve packets.
- **sample**—The following sample packet types are available:
  - **host**—Host packets.
  - **pfe**—Packet Forwarding Engine packets.
  - **syslog**—System log message packets.
  - **tap**—TAP packets.
- **tcp-flags**—The following TCP-flagged packet types are available:
  - **established**—TCP ACK and RST connection packets.
  - **initial**—TCP SYN and SYN ACK packets.
- **unclassified**—The following unclassified packet types are available:
  - **control-layer2**—Unclassified layer 2 control packets.
  - **control-v4**—Unclassified IPv4 control packets.
  - **control-v6**—Unclassified IPv6 control packets.
  - **fw-host**—Unclassified send-to-host firewall packets.
  - **host-route-v4**—Unclassified IPv4 routing protocol and host packets in traffic sent to the router local interface address for broadcast and multicast.
  - **host-route-v6**—Unclassified IPv6 routing protocol and host packets in traffic sent to the router local interface address for broadcast and multicast.
  - **mcast-copy**—Unclassified host copy (due to multicast routing) packets.
  - **other**—All unclassified packets that do not belong to another type.
- **virtual-chassis**—The following packet types are available for virtual chassis packets:
  - **control-low**—Low-priority control packets.
  - **control-high**—High-priority control packets.

- **unclassified**— All unclassified packets in the protocol group.
- **vc-packets**—All exception packets on the virtual chassis link.
- **vc-ttl-errors**—Virtual chassis TTL error packets.

***protocol-group***—(Optional) Display DDoS protection information for one of the following protocol groups:

- **amtv4**—IPv4 AMT traffic.
- **amtv6**—IPv6 AMT traffic.
- **ancp**—ANCP traffic.
- **ancpv6**—ANCPv6 traffic.
- **arp**—ARP traffic.
- **atm**—ATM traffic.
- **bfd**—BFD traffic.
- **bfdv6**—BFDv6 traffic.
- **bgp**—BGP traffic.
- **bgpv6**—BGPv6 traffic.
- **control**—Control traffic.
- **demux-autosense**—Demux autosensing traffic.
- **dhcpv4**—DHCPv4 traffic.
- **dhcpv6**—DHCPv6 traffic.
- **diameter**—Diameter and Gx-Plus traffic.
- **dns**—DNS traffic.
- **dtcp**—DTCP traffic.
- **dynamic-vlan**—Dynamic VLAN exception traffic.
- **egpv6**—EGPv6 traffic.
- **eoam**—EOAM traffic.
- **esmc**—ESMC traffic.
- **fab-probe**—Fab out probe packets.
- **filter-action**—IPv4 and IPv6 firewall filter action packets sent to the host because of reject terms in firewall filters
- **firewall-host**—Firewall send-to-host traffic.
- **frame-relay**—Frame relay traffic.
- **ftp**—FTP traffic.
- **ftpv6**—FTPv6 traffic.

- **gre**—GRE traffic.
- **icmp**—ICMP traffic.
- **igmp**—IGMP traffic
- **igmpv4v6**—IGMP v4/v6 traffic.
- **igmpv6**—IGMPv6 traffic.
- **inline-ka**—Inline service interfaces keepalive traffic.
- **inline-svcs**—Inline services traffic.
- **ip-fragments**—IP fragments traffic.
- **ip-options**—IP traffic with IP packet header options.
- **isis**—IS-IS traffic.
- **jfm**—JFM traffic.
- **keepalive**—Keepalive traffic.
- **l2pt**—Layer 2 protocol tunneling traffic.
- **l2tp**—L2TP traffic.
- **lACP**—LACP traffic.
- **ldp**—LDP traffic.
- **ldpv6**—LDPv6 traffic.
- **lldp**—LLDP traffic.
- **lmp**—LMP traffic.
- **lmpv6**—LMPv6 traffic.
- **mac-host**—Layer 2 MAC send-to-host traffic.
- **mcast-snoop**—Control traffic for multicast snooping.
- **mlp**—MLP traffic.
- **msdp**—MSDP traffic.
- **msdpv6**—MSDPv6 traffic.
- **multicast-copy**—Host copy traffic due to multicast routing.
- **mvrp**—MVRP traffic.
- **ndpv6**—NDPv6 traffic.
- **ntp**—NTP traffic.
- **oam-lfm**—OAM-LFM traffic.
- **ospf**—OSPF traffic.
- **ospfv3v6**—OSPFv3/IPv6 traffic.
- **pfe-alive**—Packet Forwarding Engine keepalive traffic

- **pim**—PIM traffic.
- **pimv6**—PIMv6 traffic.
- **pmvrp**—PMVRP traffic.
- **pos**—POS traffic.
- **ppp**—PPP traffic.
- **pppoe**—PPPoE traffic.
- **ptp**—PTP traffic.
- **pvstp**—PVSTP traffic.
- **radius**—RADIUS traffic.
- **redirect**—Traffic that triggers ICMP redirects.
- **reject**—Packets rejected by a next-hop forwarding decision.
- **rejectv6**—V6 packets rejected by a next-hop forwarding decision.
- **resolve**—Unclassified IPv4 and IPv6 resolve packets sent to the host because of a traffic request resolve action.
- **rip**—RIP traffic.
- **ripv6**—RIPv6 traffic.
- **rsvp**—RSVP traffic.
- **rsvpv6**—RSVPv6 traffic.
- **services**—Service traffic.
- **snmp**—SNMP traffic.
- **snmpv6**—SNMPv6 traffic.
- **ssh**—SSH traffic.
- **sshv6**—SSHv6 traffic.
- **stp**—STP traffic.
- **tacacs**—TACACS traffic.
- **tcp-flags**—Traffic with TCP flags.
- **telnet**—TELNET traffic.
- **telnetv6**—TELNETv6 traffic.
- **tll**—TTL traffic.
- **tunnel-fragment**—Tunnel fragments traffic.
- **unclassified**—Unclassified traffic.
- **virtual-chassis**—Virtual chassis traffic.

- **vrrp**—VRRP traffic.
- **vrrpv6**—VRRPv6 traffic.

**Required Privilege Level** view

**Related Documentation**

- [clear ddos-protection protocols on page 318](#)
- *show ddos-protection protocols culprit-flows*
- *show ddos-protection protocols flow-detection*
- [show ddos-protection protocols parameters on page 336](#)
- [show ddos-protection protocols statistics on page 343](#)
- *show ddos-protection protocols violations*

**List of Sample Output**

- [show ddos-protection protocols on page 331](#)
- [show ddos-protection protocols \(Specific Packet Type with Flow Detection Disabled\) on page 333](#)
- [show ddos-protection protocols \(Specific Packet Type with Flow Detection Enabled and Automatic\) on page 333](#)
- [show ddos-protection protocols \(Specific Packet Type with Bandwidth Violation\) on page 334](#)

**Output Fields** [Table 26 on page 327](#) lists the output fields for the **show ddos-protection protocols** command. Output fields are listed in the approximate order in which they appear.

**Table 26: show ddos-protection protocols Output Fields**

| Field Name                     | Field Description                                                                                        |
|--------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>Packet types</b>            | Number of packet types                                                                                   |
| <b>Modified</b>                | Number of packets for which policer values have been modified from the default.                          |
| <b>Received traffic</b>        | Number of traffic flows received.                                                                        |
| <b>Currently violated</b>      | Number of flows that are currently violating the flow bandwidth limit.                                   |
| <b>Currently tracked flows</b> | Number of active flows that are being tracked as culprit flows by flow detection.                        |
| <b>Total detected flows</b>    | Total number of culprit flows that have been detected, including those that have recovered or timed out. |
| <b>Protocol Group</b>          | Name of protocol group.                                                                                  |
| <b>Packet type</b>             | Name of packet type in protocol group.                                                                   |

Table 26: show ddos-protection protocols Output Fields (*continued*)

| Field Name                          | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Bandwidth</b>                    | Bandwidth policer value; number of packets per second that is allowed before a violation is declared.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Burst</b>                        | Burst policer value; the maximum number of packets that is allowed in a burst before a violation is declared.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Priority</b>                     | Priority of the packet type for individual packet policers that enables more important traffic to pass through in the event of traffic congestion: <b>low</b> , <b>medium</b> , or <b>high</b> . Lower priority packets can be dropped when insufficient bandwidth is available.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Recover time</b>                 | Time that must pass since the last violation before the traffic flow is considered to have recovered from the attack. A notification is generated when the timer expires.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Enabled</b>                      | State of the policer, enabled ( <b>Yes</b> ), disabled ( <b>No</b> ), or partially disabled ( <b>Partial</b> ); <b>Partial</b> indicates that only some of the policer instances are disabled for the policer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Bypass aggregate</b>             | <p>State of the bypass aggregate configuration:</p> <ul style="list-style-type: none"> <li>• Yes—The aggregate policer is bypassed.</li> <li>• No—The aggregate policer is enforced.</li> </ul> <p>This field appears only for individual policers.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Flow detection configuration</b> | <p>State of flow detection configured on the router:</p> <ul style="list-style-type: none"> <li>• Detection mode—Mode of operation for suspicious flow detection: automatic, off, or on.</li> <li>• Log flows—State of automatic logging of suspicious traffic flows: on (<b>Yes</b>) or off (<b>No</b>).</li> <li>• Timeout flows—State of culprit flow timeout behavior: flow is suppressed for a configured timeout period (<b>Yes</b>) or flow is suppressed until it is no longer in violation (<b>No</b>).</li> <li>• Detect time—Time in seconds that must pass before a suspicious flow that has exceeded the bandwidth allowed for the packet type is considered to be a culprit flow.</li> <li>• Recover time—Time in seconds that must pass before a culprit flow is considered to have returned to normal. The period starts when the flow drops below the threshold that triggered the last violation.</li> <li>• Timeout time—Time in seconds that a culprit flow is suppressed, if timeouts have been enabled.</li> <li>• Flow aggregation level configuration—Flow detection mode, flow control mode, and flow bandwidth for traffic at each of the traffic flow aggregation levels: subscriber, logical interface, and physical interface. <ul style="list-style-type: none"> <li>• Detection mode—State of flow detection: automatic, off, or on.</li> <li>• Control mode—Mode of controlling culprit traffic: dropped, kept, or policed back to within the allowed bandwidth.</li> <li>• Flow rate—Bandwidth allowed for the control traffic in packets per second.</li> </ul> </li> </ul> |

Table 26: show ddos-protection protocols Output Fields (*continued*)

| Field Name                        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>System-wide information</b>    | <p>The following information collected for the router:</p> <ul style="list-style-type: none"> <li>• A message indicates whether the policer has been violated.</li> <li>• No. of FPCs currently receiving excess traffic—Number of cards that are currently in violation of a policer.</li> <li>• No. of FPCs that have received excess traffic—Number of cards that have at some point been in violation of a policer.</li> <li>• Violation first detected at—Timestamp of the first violation.</li> <li>• Violation last seen at—Timestamp of the last observed violation.</li> <li>• Duration of violation—Length of the violation.</li> <li>• Number of violations—Number of times the violation has occurred.</li> <li>• Received—Number of packets received at all card slots and the Routing Engine.</li> <li>• Dropped—Number of packets dropped regardless of where they were dropped.</li> <li>• Arrival rate—Current traffic rate for packets arriving from all cards and at the Routing Engine.</li> <li>• Max arrival rate—Highest traffic rate for packets arriving from all cards and at the Routing Engine.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Routing Engine information</b> | <p>The following information collected for the Routing Engine:</p> <ul style="list-style-type: none"> <li>• Bandwidth—Maximum number of packets per second that is allowed.</li> <li>• Burst—Maximum number of packets that is allowed in a burst.</li> <li>• A message indicates the State of the policer, enabled (<b>Yes</b>) or disabled (<b>No</b>).</li> <li>• A message indicates whether the policer has been violated; the policer might be passed at the individual cards, but the combined rate of packets arriving at the Routing Engine can exceed the configured policer value.</li> <li>• Violation first detected at—Timestamp of the first violation.</li> <li>• Violation last seen at—Timestamp of the last observed violation.</li> <li>• Duration of violation—Length of the violation.</li> <li>• Number of violations—Number of times the violation has occurred.</li> <li>• Received—Number of packets received at the Routing Engine from all cards.</li> <li>• Dropped—Number of packets dropped at the Routing Engine; includes packets dropped by the aggregate policer and by individual protocol policers.</li> <li>• Arrival rate—Current traffic rate for packets arriving at the Routing Engine from all cards.</li> <li>• Max arrival rate—Highest traffic rate for packets arriving at the Routing Engine from all cards.</li> <li>• Dropped by aggregate policer—Number of packets dropped by the aggregate policer.</li> <li>• Dropped by individual policers—Number of packets dropped by individual policer.</li> </ul> |

Table 26: show ddos-protection protocols Output Fields (*continued*)

| Field Name                                  | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>FPC slot information</b>                 | <p>The following information collected for the card in the indicated slot:</p> <ul style="list-style-type: none"> <li>• Bandwidth—Bandwidth scaling percentage and the number of packets per second that is allowed before a violation is declared.</li> <li>• Burst—Burst scaling percentage and the maximum number of packets that is allowed in a burst before a violation is declared.</li> <li>• A message indicates whether the policer has been violated.</li> <li>• Violation first detected at—Timestamp of the first violation.</li> <li>• Violation last seen at—Timestamp of the last observed violation.</li> <li>• Duration of violation—Length of the violation.</li> <li>• Number of violations—Number of times the violation has occurred.</li> <li>• Received—Number of packets received on the line card.</li> <li>• Dropped—Number of packets dropped at the line card; includes packets dropped by the aggregate policer and by individual protocol policers.</li> <li>• Arrival rate—Current traffic rate for packets arriving at the line card.</li> <li>• Max arrival rate—Highest traffic rate for packets arriving at the line card.</li> <li>• Dropped by this policer—Number of packets dropped by the individual policer.</li> <li>• Dropped by aggregate policer—Number of packets dropped by the aggregate policer.</li> </ul> |
| <b>Bypass aggr.</b>                         | <p>State of the bypass aggregate configuration:</p> <ul style="list-style-type: none"> <li>• Yes—The aggregate policer configuration is bypassed.</li> <li>• No—The aggregate policer configuration is enforced.</li> </ul> <p>Dashes indicate that the bypass aggregate configuration is not available; this is possible only for aggregate policers.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>FPC Mod</b>                              | <p>Indicates whether configuration has changed from the default for any line cards.</p> <ul style="list-style-type: none"> <li>• No—The default configuration has not changed from the default for the packet type.</li> <li>• Yes—The default configuration has changed from the default for the packet type</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Op mode</b>                              | <p>Mode of operation for suspicious flow detection for the packet type: always-on (<b>on</b>), (<b>auto</b>), or disabled (<b>off</b>).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Policer BW (pps)</b>                     | <p>Bandwidth policer value; number of packets per second that is allowed before a violation is declared.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Aggr level<br/>Op:Fc:Bandwidth (pps)</b> | <p>Flow operation mode, flow control mode, and flow bandwidth for traffic of the packet type at each traffic flow aggregation level: subscriber (<b>sub</b>), logical interface (<b>ifl</b>), and physical interface (<b>ifd</b>).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Log flow</b>                             | <p>State of automatic logging of suspicious traffic flows for the packet type: on (<b>Yes</b>) or off (<b>No</b>).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |



Table 26: show ddos-protection protocols Output Fields (*continued*)

| Field Name | Field Description                                                                                                                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time out   | State of culprit flow timeout behavior for the packet type: flow is suppressed or monitored for a configured timeout period ( <b>Yes</b> ) or flow is suppressed or monitored until it is no longer in violation ( <b>No</b> ). |

## Sample Output

### show ddos-protection protocols

```
user@host> show ddos-protection protocols
```

```
Packet types: 190, Modified: 0, Received traffic: 12, Currently violated: 3
Currently tracked flows: 0, Total detected flows: 0
* = User configured value
```

```
Protocol Group: IPv4-Unclassified
```

```
Packet type: aggregate (Aggregate for unclassified host-bound IPv4 traff)
```

```
Aggregate policer configuration:
```

```
Bandwidth: 2000 pps
Burst: 10000 packets
Recover time: 300 seconds
Enabled: Yes
```

```
Flow detection configuration:
```

```
Detection mode: Automatic Detect time: 3 seconds
Log flows: No Recover time: 60 seconds
Timeout flows: No Timeout time: 300 seconds
```

```
Flow aggregation level configuration:
```

| Aggregation level  | Detection mode | Control mode | Flow rate |
|--------------------|----------------|--------------|-----------|
| Subscriber         | Automatic      | Drop         | 10 pps    |
| Logical interface  | Automatic      | Drop         | 10 pps    |
| Physical interface | Automatic      | Drop         | 2000 pps  |

```
System-wide information:
```

```
Aggregate bandwidth is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
```

```
Routing Engine information:
```

```
Bandwidth: 2000 pps, Burst: 10000 packets, enabled
Aggregate policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by individual policers: 0
```

```
FPC slot 1 information:
```

```
Bandwidth: 100% (2000 pps), Burst: 100% (10000 packets), enabled
Aggregate policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by individual policers: 0
Dropped by flow suppression: 0
```

```
...
```

```
Protocol Group: PPPoE
```

```
Packet type: aggregate (Aggregate for all PPPoE control traffic)
```

```
Aggregate policer configuration:
```

```

Bandwidth: 2000 pps
Burst: 2000 packets
Recover time: 300 seconds
Enabled: Yes
Flow detection configuration:
Detection mode: Automatic Detect time: 3 seconds
Log flows: No Recover time: 60 seconds
Timeout flows: No Timeout time: 300 seconds
Flow aggregation level configuration:
 Aggregation level Detection mode Control mode Flow rate
 Subscriber Automatic Drop 10 pps
 Logical interface Automatic Drop 10 pps
 Physical interface Automatic Drop 2000 pps
System-wide information:
Aggregate bandwidth is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Routing Engine information:
Bandwidth: 2000 pps, Burst: 2000 packets, enabled
Aggregate policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by individual policers: 0
FPC slot 1 information:
Bandwidth: 100% (2000 pps), Burst: 100% (2000 packets), enabled
Aggregate policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by individual policers: 0
Dropped by flow suppression: 0

Packet type: padi (PPPoE PADI)
Individual policer configuration:
Bandwidth: 500 pps
Burst: 500 packets
Priority: Low
Recover time: 300 seconds
Enabled: Yes
Bypass aggregate: No
Flow detection configuration:
Detection mode: Automatic Detect time: 3 seconds
Log flows: No Recover time: 60 seconds
Timeout flows: No Timeout time: 300 seconds
Flow aggregation level configuration:
 Aggregation level Detection mode Control mode Flow rate
 Subscriber Automatic Drop 10 pps
 Logical interface Automatic Drop 10 pps
 Physical interface Automatic Drop 500 pps
System-wide information:
Bandwidth is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Routing Engine information:
Bandwidth: 500 pps, Burst: 500 packets, enabled
Policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
Policer is never violated

```

```

Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by aggregate policer: 0
Dropped by flow suppression: 0
...

```

### show ddos-protection protocols (Specific Packet Type with Flow Detection Disabled)

```

user@host> show ddos-protection protocols pppoe padi
Currently tracked flows: 0, Total detected flows: 0
* = User configured value

Protocol Group: PPPoE

Packet type: padi (PPPoE PADI)
Individual policer configuration:
 Bandwidth: 500 pps
 Burst: 500 packets
 Priority: Low
 Recover time: 300 seconds
 Enabled: Yes
 Bypass aggregate: No
Flow detection configuration:
 Detection mode: Off* Detect time: 3 seconds
 Log flows: No Recover time: 60 seconds
 Timeout flows: No Timeout time: 300 seconds
Flow aggregation level configuration:
 Aggregation level Detection mode Control mode Flow rate
 Subscriber Automatic Drop 10 pps
 Logical interface Automatic Drop 10 pps
 Physical interface Automatic Drop 500 pps
System-wide information:
 Bandwidth is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
Routing Engine information:
 Bandwidth: 500 pps, Burst: 500 packets, enabled
 Policer is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
 Dropped by aggregate policer: 0
FPC slot 1 information:
 Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
 Policer is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
 Dropped by aggregate policer: 0
 Dropped by flow suppression: 0

```

### show ddos-protection protocols (Specific Packet Type with Flow Detection Enabled and Automatic)

```

user@host> show ddos-protection protocols pppoe padi
Currently tracked flows: 0, Total detected flows: 0
* = User configured value

```

Protocol Group: PPPoE

```

Packet type: padi (PPPoE PADI)
Individual policer configuration:
 Bandwidth: 500 pps
 Burst: 500 packets

```

```

Priority: Low
Recover time: 300 seconds
Enabled: Yes
Bypass aggregate: No
Flow detection configuration:
 Detection mode: Automatic Detect time: 3 seconds
 Log flows: No Recover time: 60 seconds
 Timeout flows: No Timeout time: 300 seconds
Flow aggregation level configuration:
 Aggregation level Detection mode Control mode Flow rate
 Subscriber Automatic Drop 10 pps
 Logical interface Automatic Drop 10 pps
 Physical interface Automatic Drop 500 pps
System-wide information:
 Bandwidth is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
Routing Engine information:
 Bandwidth: 500 pps, Burst: 500 packets, enabled
 Policer is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
 Dropped by aggregate policer: 0
FPC slot 1 information:
 Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
 Policer is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
 Dropped by aggregate policer: 0
 Dropped by flow suppression: 0

```

### show ddos-protection protocols (Specific Packet Type with Bandwidth Violation)

```

user@host> show ddos-protection protocols bfd
Packet types: 1, Modified: 0, Received traffic: 1, Currently violated: 1
Currently tracked flows: 1, Total detected flows: 1
* = User configured value

```

Protocol Group: BFD

```

Packet type: aggregate (Aggregate for all bfd traffic)
Aggregate policer configuration:
 Bandwidth: 20000 pps
 Burst: 20000 packets
 Recover time: 300 seconds
 Enabled: Yes
Flow detection configuration:
 Detection mode: Automatic Detect time: 3 seconds
 Log flows: No Recover time: 60 seconds
 Timeout flows: No Timeout time: 300 seconds
Flow aggregation level configuration:
 Aggregation level Detection mode Control mode Flow rate
 Subscriber Automatic Drop 10 pps
 Logical interface Automatic Drop 10 pps
 Physical interface Automatic Drop 20000 pps
System-wide information:
 Aggregate bandwidth is being violated!
 No. of FPCs currently receiving excess traffic: 1
 No. of FPCs that have received excess traffic: 1
 Violation first detected at: 2012-10-24 23:40:20 EDT
 Violation last seen at: 2012-10-25 10:25:48 EDT

```

Duration of violation: 10:45:28 Number of violations: 1  
 Received: 1173471731 Arrival rate: 30304 pps  
 Dropped: 399135607 Max arrival rate: 30331 pps  
 Flow counts:

|                   |         |                |
|-------------------|---------|----------------|
| Aggregation level | Current | Total detected |
| Subscriber        | 1       | 1              |
| Total             | 1       | 1              |

Routing Engine information:  
 Bandwidth: 20000 pps, Burst: 20000 packets, enabled  
 Aggregate policer is never violated  
 Received: 366831604 Arrival rate: 0 pps  
 Dropped: 0 Max arrival rate: 9522 pps  
 Dropped by individual policers: 0

**FPC slot 1 information:**  
**Bandwidth: 100% (20000 pps), Burst: 100% (20000 packets), enabled**  
**Aggregate policer is currently being violated!**  
 Violation first detected at: 2012-10-24 23:40:21 EDT  
 Violation last seen at: 2012-10-25 10:25:48 EDT  
 Duration of violation: 10:45:27 Number of violations: 1  
 Received: 1173471731 Arrival rate: 30304 pps  
 Dropped: 399135607 Max arrival rate: 30331 pps  
 Dropped by individual policers: 0  
 Dropped by aggregate policer: 398854530  
 Dropped by flow suppression: 281077

Flow counts:

|                    |         |                |        |
|--------------------|---------|----------------|--------|
| Aggregation level  | Current | Total detected | State  |
| Subscriber         | 1       | 1              | Active |
| Logical-interface  | 0       | 0              | Active |
| Physical-interface | 0       | 0              | Active |
| Total              | 1       | 1              |        |

## show ddos-protection protocols parameters

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show ddos-protection protocols &lt;protocol-group&gt; parameters</code><br><code>&lt;brief   detail   terse&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.2.<br>Command introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Display DDoS protection configuration information for all protocol groups or for a particular protocol group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Options</b>                  | <p><b>none</b>—Display information for all protocol groups.</p> <p><b>brief   detail   terse</b>—(Optional) Display the specified level of output.</p> <ul style="list-style-type: none"> <li><b>brief</b>—Display basic function information.</li> <li><b>detail</b>—Add information to the <b>brief</b> output; it is identical to the output displayed when you choose no option. The <b>brief</b> and <b>detail</b> options display information for all protocol groups, which can be a long list.</li> <li><b>terse</b>—Display the same level of information as the <b>brief</b> option but only for active protocol groups—groups that show traffic in the <b>Received (packets)</b> column.</li> </ul> <p><b>protocol-group</b>—(Optional) Display information for a particular protocol group. See <a href="#">show ddos-protection protocols</a> for a list of available groups on platforms other than QFX5100. See <a href="#">protocols</a> for a list of available groups on QFX5100.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">clear ddos-protection protocols on page 318</a></li> <li><a href="#">show ddos-protection protocols on page 320</a></li> <li><a href="#">show ddos-protection protocols culprit-flows</a></li> <li><a href="#">show ddos-protection protocols flow-detection</a></li> <li><a href="#">show ddos-protection protocols statistics on page 343</a></li> <li><a href="#">show ddos-protection protocols violations</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection protocols parameters on page 338</a><br><a href="#">show ddos-protection protocols parameters brief on page 339</a><br><a href="#">show ddos-protection protocols dhcpv4 parameters brief on page 340</a><br><a href="#">show ddos-protection protocols dhcpv4 parameters terse on page 341</a><br><a href="#">show ddos-protection protocols dhcpv4 parameters on page 341</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Output Fields</b>            | Table 27 on <a href="#">page 337</a> lists the output fields for the <b>show ddos-protection protocols parameters</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

Table 27: show ddos-protection protocols parameters Output Fields

| Field Name                  | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                     | Level of Output    |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>Protocol Group</b>       | Name of protocol group.                                                                                                                                                                                                                                                                                                                                                                                                                               | All levels         |
| <b>Packet type</b>          | Name of packet type in protocol group.                                                                                                                                                                                                                                                                                                                                                                                                                | All levels         |
| <b>Bandwidth</b>            | Bandwidth policer value; number of packets per second that is allowed before a violation is declared.<br><br>In the <b>brief</b> output, an asterisk indicates the value has been modified from the default.                                                                                                                                                                                                                                          | All levels         |
| <b>Burst</b>                | Burst policer value; the maximum number of packets that is allowed in a burst before a violation is declared.<br><br>In the <b>brief</b> output, an asterisk indicates the value has been modified from the default.                                                                                                                                                                                                                                  | All levels         |
| <b>Priority</b>             | Priority of the packet type in the event of traffic congestion: <b>low</b> , <b>medium</b> , or <b>high</b> . Lower priority packets can be dropped when insufficient bandwidth is available.<br><br>In the <b>brief</b> output, an asterisk indicates the value has been modified from the default.<br><br><b>NOTE:</b> Packet-type policers are not supported on QFX5100 switches.                                                                  | All levels         |
| <b>Recover time</b>         | Time that must pass since the last violation before the traffic flow is considered to have recovered from the attack. A notification is generated when the timer expires.<br><br>In the <b>brief</b> output, an asterisk indicates the value has been modified from the default.                                                                                                                                                                      | All levels         |
| <b>Enabled</b>              | State of the policer, enabled ( <b>Yes</b> ) or disabled ( <b>No</b> ).                                                                                                                                                                                                                                                                                                                                                                               | <b>detail none</b> |
| <b>Bypass aggregate</b>     | State of the bypass aggregate configuration:<br><ul style="list-style-type: none"> <li>• Yes—The aggregate policer is bypassed.</li> <li>• No—The aggregate policer is enforced.</li> </ul> This field appears only for individual policers.<br><br><b>NOTE:</b> Packet-type policers are not supported on QFX5100 switches.                                                                                                                          | <b>detail none</b> |
| <b>FPC slot information</b> | The following configuration information for the card in the indicated slot:<br><ul style="list-style-type: none"> <li>• Bandwidth—Bandwidth scale and the number of packets per second that is allowed before a violation is declared</li> <li>• Burst—Burst scale and the maximum number of packets that is allowed in a burst before a violation is declared</li> <li>• <b>enabled</b> or <b>disabled</b>—State of the line card policer</li> </ul> | <b>detail none</b> |

Table 27: show ddos-protection protocols parameters Output Fields (*continued*)

| Field Name                         | Field Description                                                                                                                                                                                                                                                                                                                                                                                       | Level of Output    |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>Number of policers modified</b> | Number of policers that have been changed from the default configuration.<br><br>An asterisk by a particular value indicates that value has been modified.                                                                                                                                                                                                                                              | <b>brief terse</b> |
| <b>Policer Enabled</b>             | State of the policer, enabled ( <b>Yes</b> ), disabled ( <b>No</b> ), or partially disabled ( <b>part.</b> ); <b>part.</b> indicates that only some of the policer instances are disabled for the policer.                                                                                                                                                                                              | <b>brief terse</b> |
| <b>Bypass aggr.</b>                | State of the bypass aggregate configuration:<br><br><ul style="list-style-type: none"> <li>• Yes—The aggregate policer is bypassed.</li> <li>• No—The aggregate policer is enforced.</li> </ul> Dashes indicate that the bypass aggregate configuration is not available; this is possible only for aggregate policers.<br><br><b>NOTE:</b> Packet-type policers are not supported on QFX5100 switches. | <b>brief terse</b> |
| <b>FPC Mod</b>                     | Indicates whether configuration has changed from the default for any line cards.<br><br><ul style="list-style-type: none"> <li>• No—The default configuration has not changed from the default for the packet type.</li> <li>• Yes—The default configuration has changed from the default for the packet type</li> </ul>                                                                                | <b>brief terse</b> |

## Sample Output

### show ddos-protection protocols parameters

```

user@host> show ddos-protection protocols parameters
Protocol Group: IPv4-Unclassified

Packet type: aggregate (Aggregate for unclassified host-bound IPv4 traffic)
Aggregate policer configuration:
 Bandwidth: 20000 pps
 Burst: 20000 packets
 Priority: medium
 Recover time: 300 seconds
 Enabled: Yes
FPC slot 1 information:
 Bandwidth: 100% (20000 pps), Burst: 100% (20000 packets), enabled

Protocol Group: IPv6-Unclassified

Packet type: aggregate (Aggregate for unclassified host-bound IPv6 traffic)
Aggregate policer configuration:
 Bandwidth: 20000 pps
 Burst: 20000 packets
 Priority: medium
 Recover time: 300 seconds
 Enabled: Yes
FPC slot 1 information:
 Bandwidth: 100% (20000 pps), Burst: 100% (20000 packets), enabled

...

```



## Protocol Group: PPPoE

Packet type: aggregate (Aggregate for all PPPoE control traffic)

Aggregate policer configuration:

Bandwidth: 800 pps  
Burst: 2000 packets  
Priority: medium  
Recover time: 300 seconds  
Enabled: Yes

FPC slot 1 information:

Bandwidth: 100% (800 pps), Burst: 100% (2000 packets), enabled

Packet type: padi (PPPoE PADI)

Individual policer configuration:

Bandwidth: 500 pps  
Burst: 500 packets  
Priority: low  
Recover time: 300 seconds  
Enabled: Yes

Bypass aggregate: No

FPC slot 1 information:

Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled

Packet type: pado (PPPoE PADO)

Individual policer configuration:

Bandwidth: 0 pps  
Burst: 0 packets  
Priority: low  
Recover time: 300 seconds  
Enabled: Yes

Bypass aggregate: No

FPC slot 1 information:

Bandwidth: 100% (0 pps), Burst: 100% (0 packets), enabled

Packet type: padr (PPPoE PADR)

Individual policer configuration:

Bandwidth: 500 pps  
Burst: 500 packets  
Priority: medium  
Recover time: 300 seconds  
Enabled: Yes

Bypass aggregate: No

FPC slot 1 information:

Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled

## show ddos-protection protocols parameters brief

user@host> show ddos-protection protocols parameters brief

Number of policers modified: 3

| Protocol group | Packet type | Bandwidth (pps) | Burst (pkts) | Priority | Recover time(sec) | Policer enabled | Bypass aggr. | FPC mod |
|----------------|-------------|-----------------|--------------|----------|-------------------|-----------------|--------------|---------|
| ipv4-uncls     | aggregate   | 20000           | 20000        | medium   | 300               | yes             | --           | no      |
| ipv6-uncls     | aggregate   | 20000           | 20000        | medium   | 300               | yes             | --           | no      |
| dynvlan        | aggregate   | 1000            | 500          | low      | 300               | yes             | --           | no      |
| ppp            | aggregate   | 16000           | 16000        | medium   | 300               | yes             | --           | no      |
| ppp            | unclass     | 1000            | 500          | low      | 300               | yes             | no           | no      |
| ppp            | lcp         | 12000           | 12000        | low      | 300               | yes             | no           | no      |
| ppp            | auth        | 2000            | 2000         | medium   | 300               | yes             | no           | no      |
| ppp            | ipcp        | 2000            | 2000         | high     | 300               | yes             | no           | no      |
| ppp            | ipv6cp      | 2000            | 2000         | high     | 300               | yes             | no           | no      |

|         |            |       |       |        |     |        |    |    |
|---------|------------|-------|-------|--------|-----|--------|----|----|
| ppp     | mplscp     | 2000  | 2000  | high   | 300 | yes    | no | no |
| ppp     | isis       | 2000  | 2000  | high   | 300 | yes    | no | no |
| pppoe   | aggregate  | 800*  | 2000  | medium | 300 | part.* | -- | no |
| pppoe   | padi       | 500   | 500   | low    | 300 | part.  | no | no |
| pppoe   | pado       | 0     | 0     | low    | 300 | part.  | no | no |
| pppoe   | padr       | 500   | 500   | medium | 300 | part.  | no | no |
| pppoe   | pads       | 0     | 0     | low    | 300 | part.  | no | no |
| pppoe   | padt       | 1000  | 1000  | high   | 300 | part.  | no | no |
| pppoe   | padm       | 0     | 0     | low    | 300 | part.  | no | no |
| pppoe   | padn       | 0     | 0     | low    | 300 | part.  | no | no |
| dhcipv4 | aggregate  | 669*  | 5000  | medium | 300 | yes    | -- | no |
| dhcipv4 | unclass..  | 300   | 150   | low    | 300 | yes    | no | no |
| dhcipv4 | discover   | 100*  | 500   | low    | 300 | yes    | no | no |
| dhcipv4 | offer      | 1000  | 1000  | low    | 300 | yes    | no | no |
| dhcipv4 | request    | 1000  | 1000  | medium | 300 | yes    | no | no |
| dhcipv4 | decline    | 500   | 500   | low    | 300 | yes    | no | no |
| dhcipv4 | ack        | 500   | 500   | medium | 300 | yes    | no | no |
| dhcipv4 | nak        | 500   | 500   | low    | 300 | yes    | no | no |
| dhcipv4 | release    | 2000  | 2000  | high   | 300 | yes    | no | no |
| dhcipv4 | inform     | 500   | 500   | low    | 300 | yes    | no | no |
| dhcipv4 | renew      | 2000  | 2000  | high   | 300 | yes    | no | no |
| dhcipv4 | forcerenew | 2000  | 2000  | high   | 300 | yes    | no | no |
| dhcipv4 | leasequery | 2000  | 2000  | high   | 300 | yes    | no | no |
| dhcipv4 | leaseuna.. | 2000  | 2000  | high   | 300 | yes    | no | no |
| dhcipv4 | leaseunk.. | 2000  | 2000  | high   | 300 | yes    | no | no |
| dhcipv4 | leaseact.. | 2000  | 2000  | high   | 300 | yes    | no | no |
| dhcipv4 | bootp      | 300   | 300   | low    | 300 | yes    | no | no |
| dhcipv4 | no-msgtype | 0     | 0     | low    | 300 | yes    | no | no |
| dhcipv4 | bad-pack.. | 0     | 0     | low    | 300 | yes    | no | no |
| ...     |            |       |       |        |     |        |    |    |
| icmp    | aggregate  | 20000 | 20000 | high   | 300 | yes    | -- | no |
| igmp    | aggregate  | 20000 | 20000 | high   | 300 | yes    | -- | no |
| ospf    | aggregate  | 20000 | 20000 | high   | 300 | yes    | -- | no |
| rsvp    | aggregate  | 20000 | 20000 | high   | 300 | yes    | -- | no |
| pim     | aggregate  | 20000 | 20000 | high   | 300 | yes    | -- | no |
| rip     | aggregate  | 20000 | 20000 | high   | 300 | yes    | -- | no |
| ptp     | aggregate  | 20000 | 20000 | high   | 300 | yes    | -- | no |
| bfd     | aggregate  | 20000 | 20000 | high   | 300 | yes    | -- | no |
| lmp     | aggregate  | 20000 | 20000 | high   | 300 | yes    | -- | no |
| ldp     | aggregate  | 20000 | 20000 | high   | 300 | yes    | -- | no |
| msdp    | aggregate  | 20000 | 20000 | high   | 300 | yes    | -- | no |
| bgp     | aggregate  | 20000 | 20000 | low    | 300 | yes    | -- | no |
| vrrp    | aggregate  | 20000 | 20000 | high   | 300 | yes    | -- | no |
| telnet  | aggregate  | 20000 | 20000 | low    | 300 | yes    | -- | no |
| ftp     | aggregate  | 20000 | 20000 | low    | 300 | yes    | -- | no |
| ssh     | aggregate  | 20000 | 20000 | low    | 300 | yes    | -- | no |
| snmp    | aggregate  | 20000 | 20000 | low    | 300 | yes    | -- | no |
| ancp    | aggregate  | 20000 | 20000 | low    | 300 | yes    | -- | no |
| ...     |            |       |       |        |     |        |    |    |

#### show ddos-protection protocols dhcipv4 parameters brief

```

user@host> show ddos-protection protocols dhcipv4 parameters brief
Number of policers modified: 2
Protocol Packet Bandwidth Burst Priority Recover Policer Bypass FPC
group type (pps) (pkts) time(sec) enabled aggr. mod
dhcipv4 aggregate 669* 5000 medium 300 yes -- no
dhcipv4 unclass.. 300 150 low 300 yes no no

```

|        |            |      |      |        |     |     |    |    |
|--------|------------|------|------|--------|-----|-----|----|----|
| dhcpv4 | discover   | 100* | 500  | low    | 300 | yes | no | no |
| dhcpv4 | offer      | 1000 | 1000 | low    | 300 | yes | no | no |
| dhcpv4 | request    | 1000 | 1000 | medium | 300 | yes | no | no |
| dhcpv4 | decline    | 500  | 500  | low    | 300 | yes | no | no |
| dhcpv4 | ack        | 500  | 500  | medium | 300 | yes | no | no |
| dhcpv4 | nak        | 500  | 500  | low    | 300 | yes | no | no |
| dhcpv4 | release    | 2000 | 2000 | high   | 300 | yes | no | no |
| dhcpv4 | inform     | 500  | 500  | low    | 300 | yes | no | no |
| dhcpv4 | renew      | 2000 | 2000 | high   | 300 | yes | no | no |
| dhcpv4 | forcerenew | 2000 | 2000 | high   | 300 | yes | no | no |
| dhcpv4 | leasequery | 2000 | 2000 | high   | 300 | yes | no | no |
| dhcpv4 | leaseuna.. | 2000 | 2000 | high   | 300 | yes | no | no |
| dhcpv4 | leaseunk.. | 2000 | 2000 | high   | 300 | yes | no | no |
| dhcpv4 | leaseact.. | 2000 | 2000 | high   | 300 | yes | no | no |
| dhcpv4 | bootp      | 300  | 300  | low    | 300 | yes | no | no |
| dhcpv4 | no-msgtype | 0    | 0    | low    | 300 | yes | no | no |
| dhcpv4 | bad-pack.. | 0    | 0    | low    | 300 | yes | no | no |

### show ddos-protection protocols dhcpv4 parameters terse

```

user@host> show ddos-protection protocols dhcpv4 parameters terse
Number of policers modified: 2
Protocol Packet Bandwidth Burst Priority Recover Policer Bypass FPC
group type (pps) (pkts) time(sec) enabled aggr. mod
dhcpv4 aggregate 669* 5000 medium 300 yes -- no
dhcpv4 discover 100* 500 low 300 yes no no

```

### show ddos-protection protocols dhcpv4 parameters

```

user@host> show ddos-protection protocols dhcpv4 parameters
Protocol Group: DHCPv4

Packet type: aggregate (aggregate for all DHCPv4 traffic)
Aggregate policer configuration:
 Bandwidth: 669 pps
 Burst: 5000 packets
 Priority: medium
 Recover time: 300 seconds
 Enabled: Yes
FPC slot 1 information:
 Bandwidth: 100% (669 pps), Burst: 100% (5000 packets), enabled

Packet type: unclassified (Unclassified DHCPv4 traffic)
Individual policer configuration:
 Bandwidth: 300 pps
 Burst: 150 packets
 Priority: low
 Recover time: 300 seconds
 Enabled: Yes
 Bypass aggregate: No
FPC slot 1 information:
 Bandwidth: 100% (300 pps), Burst: 100% (150 packets), enabled

Packet type: discover (DHCPv4 DHCPDISCOVER)
Individual policer configuration:
 Bandwidth: 100 pps
 Burst: 500 packets
 Priority: low
 Recover time: 300 seconds
 Enabled: Yes
 Bypass aggregate: No

```

FPC slot 1 information:

Bandwidth: 100% (100 pps), Burst: 100% (500 packets), enabled

Packet type: offer (DHCPv4 DHCPOFFER)

Individual policer configuration:

Bandwidth: 1000 pps

Burst: 1000 packets

Priority: low

Recover time: 300 seconds

Enabled: Yes

Bypass aggregate: No

FPC slot 1 information:

Bandwidth: 100% (1000 pps), Burst: 100% (1000 packets), enabled

Packet type: request (DHCPv4 DHCPREQUEST)

Individual policer configuration:

Bandwidth: 1000 pps

Burst: 1000 packets

Priority: medium

Recover time: 300 seconds

Enabled: Yes

Bypass aggregate: No

FPC slot 1 information:

Bandwidth: 100% (1000 pps), Burst: 100% (1000 packets), enabled

...

## show ddos-protection protocols statistics

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show ddos-protection protocols &lt;protocol-group&gt; statistics</code><br><code>&lt;brief   detail   terse&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.2.<br>Command introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | Display traffic statistics and DDoS policer violation statistics for all protocol groups or for a particular protocol group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Options</b>                  | <p><b>none</b>—Display information for all protocol groups.</p> <p><b>brief   detail   terse</b>—(Optional) Display the specified level of output.</p> <ul style="list-style-type: none"> <li><b>brief</b>—Display basic function information.</li> <li><b>detail</b>—Add information to the <b>brief</b> output; it is identical to the output displayed when you choose no option. The <b>brief</b> and <b>detail</b> options display information for all protocol groups, which can be a long list.</li> <li><b>terse</b>—Display the same level of information as the <b>brief</b> option but only for active protocol groups—groups that show traffic in the <b>Received (packets)</b> column.</li> </ul> <p><b>protocol-group</b>—(Optional) Display information for a particular protocol group. See <a href="#">show ddos-protection protocols</a> for a list of available groups on platforms other than QFX5100. See <a href="#">protocols</a> for a list of available groups on QFX5100.</p> |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li><a href="#">clear ddos-protection protocols on page 318</a></li> <li><a href="#">show ddos-protection protocols on page 320</a></li> <li><i>show ddos-protection protocols culprit-flows</i></li> <li><i>show ddos-protection protocols flow-detection</i></li> <li><a href="#">show ddos-protection protocols parameters on page 336</a></li> <li><i>show ddos-protection protocols violations</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection protocols statistics on page 345</a><br><a href="#">show ddos-protection protocols statistics brief on page 348</a><br><a href="#">show ddos-protection protocols statistics terse on page 349</a><br><a href="#">show ddos-protection protocols pppoe statistics on page 350</a><br><a href="#">show ddos-protection protocols pppoe statistics brief on page 352</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Output Fields</b>            | Table 28 on page 344 lists the output fields for the <b>show ddos-protection protocols statistics</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

Table 28: show ddos-protection protocols statistics Output Fields

| Field Name                        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Level of Output    |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>Protocol Group</b>             | Name of protocol group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | All levels         |
| <b>Packet type</b>                | Name of packet type in protocol group.<br><br><i>NOTE:</i> Packet-type policers are not supported on QFX5100 switches.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | All levels         |
| <b>System-wide information</b>    | <p>The following information collected for the router or switch:</p> <ul style="list-style-type: none"> <li>• A message indicates whether the policer has been violated.</li> <li>• No. of FPCs currently receiving excess traffic—Number of cards that are currently in violation of a policer.</li> <li>• No. of FPCs that have received excess traffic—Number of cards that have at some point been in violation of a policer.</li> <li>• Violation first detected at—Timestamp of the first violation.</li> <li>• Violation last seen at—Timestamp of the last observed violation.</li> <li>• Duration of violation—Length of the violation.</li> <li>• Number of violations—Number of times the violation has occurred.</li> <li>• Received—Number of packets received at all card slots and the Routing Engine.</li> <li>• Dropped—Number of packets dropped regardless of where they were dropped.</li> <li>• Arrival rate—Current traffic rate for packets arriving from all cards and at the Routing Engine.</li> <li>• Max arrival rate—Highest traffic rate for packets arriving from all cards and at the Routing Engine.</li> </ul>                                                                                                                                                      | <b>detail none</b> |
| <b>Routing Engine information</b> | <p>The following information collected for the Routing Engine:</p> <ul style="list-style-type: none"> <li>• A message indicates whether the policer has been violated; the policer might be passed at the individual cards, but the combined rate of packets arriving at the Routing Engine can exceed the configured policer value.</li> <li>• Violation first detected at—Timestamp of the first violation.</li> <li>• Violation last seen at—Timestamp of the last observed violation.</li> <li>• Duration of violation—Length of the violation.</li> <li>• Number of violations—Number of times the violation has occurred.</li> <li>• Received—Number of packets received at the Routing Engine from all cards.</li> <li>• Dropped—Number of packets dropped at the Routing Engine; includes packets dropped by the aggregate policer and by individual protocol policers.</li> <li>• Arrival rate—Current traffic rate for packets arriving at the Routing Engine from all cards.</li> <li>• Max arrival rate—Highest traffic rate for packets arriving at the Routing Engine from all cards.</li> <li>• Dropped by aggregate policer—Number of packets dropped by the aggregate policer.</li> <li>• Dropped by individual policers—Number of packets dropped by individual policer.</li> </ul> | <b>detail none</b> |

Table 28: show ddos-protection protocols statistics Output Fields (*continued*)

| Field Name                  | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Level of Output    |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>FPC slot information</b> | <p>The following information collected for the card in the indicated slot:</p> <ul style="list-style-type: none"> <li>• A message indicates whether the policer has been violated</li> <li>• Violation first detected at—Timestamp of the first violation</li> <li>• Violation last seen at—Timestamp of the last observed violation</li> <li>• Duration of violation—Length of the violation</li> <li>• Number of violations—Number of times the violation has occurred</li> <li>• Received—Number of packets received on the line card</li> <li>• Dropped—Number of packets dropped at the line card; includes packets dropped by the aggregate policer and by individual protocol policers</li> <li>• Arrival rate—Current traffic rate for packets arriving at the line card</li> <li>• Max arrival rate—Highest traffic rate for packets arriving at the line card</li> <li>• Dropped by this policer—Number of packets dropped by the individual policer</li> <li>• Dropped by aggregate policer—Number of packets dropped by the aggregate policer</li> </ul> | <b>detail none</b> |
| <b>Received (packets)</b>   | Number of packets of this packet type or protocol group received at all cards and the Routing Engine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>brief terse</b> |
| <b>Dropped (packets)</b>    | Number of packets dropped for this packet type or protocol group, regardless of where the packets were dropped.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>brief terse</b> |
| <b>Rate (pps)</b>           | Highest observed traffic rate for this packet type or protocol group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>brief terse</b> |
| <b>Violation counts</b>     | Number of violations of the policer bandwidth.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>brief terse</b> |
| <b>State</b>                | <p>Violation state of the packet type:</p> <ul style="list-style-type: none"> <li>• <b>ok</b>—Policer has not been violated for this packet type</li> <li>• <b>viol</b>—Policer has been violated for this packet type</li> </ul> <p><b>NOTE:</b> Packet-type policers are not supported on QFX5100 switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>brief terse</b> |

## Sample Output

### show ddos-protection protocols statistics

```

user@host> show ddos-protection protocols statistics
Protocol Group: IPv4-Unclassified

Packet type: aggregate
System-wide information:
Aggregate bandwidth is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Routing Engine information:
Aggregate policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by individual policers: 0

```

```
FPC slot 1 information:
Aggregate policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by individual policers: 0
```

Protocol Group: IPv6-Unclassified

```
Packet type: aggregate
System-wide information:
Aggregate bandwidth is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Routing Engine information:
Aggregate policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by individual policers: 0
FPC slot 1 information:
Aggregate policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by individual policers: 0
```

Protocol Group: PPPoE

```
Packet type: aggregate
System-wide information:
Aggregate bandwidth is never violated
Received: 61961244 Arrival rate: 4000 pps
Dropped: 0 Max arrival rate: 4002 pps
Routing Engine information:
Aggregate policer is never violated
Received: 15488871 Arrival rate: 1001 pps
Dropped: 0 Max arrival rate: 1011 pps
Dropped by individual policers: 0
FPC slot 1 information:
Aggregate policer is never violated
Received: 61961244 Arrival rate: 4000 pps
Dropped: 46473017 Max arrival rate: 4002 pps
Dropped by individual policers: 46473017
```

```
Packet type: padi
System-wide information:
Bandwidth is being violated!
No. of FPCs currently receiving excess traffic: 1
No. of FPCs that have received excess traffic: 1
Violation first detected at: 2011-04-19 08:23:17 PDT
Violation last seen at: 2011-04-19 12:41:23 PDT
Duration of violation: 04:18:06 Number of violations: 1
Received: 30980622 Arrival rate: 2000 pps
Dropped: 23236505 Max arrival rate: 2001 pps
Routing Engine information:
Policer is never violated
Received: 7744433 Arrival rate: 500 pps
Dropped: 0 Max arrival rate: 505 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Policer is currently being violated!
Violation first detected at: 2011-04-19 08:23:17 PDT
```



Violation last seen at: 2011-04-19 12:41:23 PDT  
 Duration of violation: 04:18:06 Number of violations: 1  
 Received: 30980622 Arrival rate: 2000 pps  
 Dropped: 23236505 Max arrival rate: 2001 pps  
 Dropped by this policer: 23236505  
 Dropped by aggregate policer: 0

Packet type: pado

System-wide information:

Bandwidth is never violated

Received: 0 Arrival rate: 0 pps  
 Dropped: 0 Max arrival rate: 0 pps

Routing Engine information:

Policer is never violated

Received: 0 Arrival rate: 0 pps  
 Dropped: 0 Max arrival rate: 0 pps

Dropped by aggregate policer: 0

FPC slot 1 information:

Policer is never violated

Received: 0 Arrival rate: 0 pps  
 Dropped: 0 Max arrival rate: 0 pps

Dropped by aggregate policer: 0

Packet type: padr

System-wide information:

Bandwidth is being violated!

No. of FPCs currently receiving excess traffic: 1

No. of FPCs that have received excess traffic: 1

Violation first detected at: 2011-04-19 08:23:17 PDT

Violation last seen at: 2011-04-19 12:43:23 PDT

Duration of violation: 04:20:06 Number of violations: 1

Received: 31220846 Arrival rate: 2000 pps  
 Dropped: 23416690 Max arrival rate: 2001 pps

Routing Engine information:

Policer is never violated

Received: 7806417 Arrival rate: 499 pps  
 Dropped: 0 Max arrival rate: 506 pps

Dropped by aggregate policer: 0

FPC slot 1 information:

Policer is currently being violated!

Violation first detected at: 2011-04-19 08:23:17 PDT

Violation last seen at: 2011-04-19 12:43:23 PDT

Duration of violation: 04:20:06 Number of violations: 1

Received: 31220846 Arrival rate: 2000 pps  
 Dropped: 23416690 Max arrival rate: 2001 pps

Dropped by this policer: 23416690

Dropped by aggregate policer: 0

Packet type: pads

System-wide information:

Bandwidth is never violated

Received: 0 Arrival rate: 0 pps  
 Dropped: 0 Max arrival rate: 0 pps

Routing Engine information:

Policer is never violated

Received: 0 Arrival rate: 0 pps  
 Dropped: 0 Max arrival rate: 0 pps

Dropped by aggregate policer: 0

FPC slot 1 information:

Policer is never violated

Received: 0 Arrival rate: 0 pps

```

Dropped: 0 Max arrival rate: 0 pps
Dropped by aggregate policer: 0

Packet type: padt
System-wide information:
Bandwidth is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Routing Engine information:
Policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by aggregate policer: 0

Packet type: padm
System-wide information:
Bandwidth is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Routing Engine information:
Policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by aggregate policer: 0

Packet type: padn
System-wide information:
Bandwidth is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Routing Engine information:
Policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Policer is never violated
Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by aggregate policer: 0

```

...

#### show ddos-protection protocols statistics brief

```
user@host> show ddos-protection protocols statistics brief
```

| Protocol group | Packet type | Received (packets) | Dropped (packets) | Rate (pps) | Violation counts | State |
|----------------|-------------|--------------------|-------------------|------------|------------------|-------|
| ipv4-unc1s     | aggregate   | 0                  | 0                 | 0          | 0                | ok    |
| ipv6-unc1s     | aggregate   | 0                  | 0                 | 0          | 0                | ok    |

```

dynvlan aggregate 0 0 0 0 ok
ppp aggregate 0 0 0 0 ok
ppp unclass 0 0 0 0 ok
ppp lcp 0 0 0 0 ok
ppp auth 0 0 0 0 ok
ppp ipcp 0 0 0 0 ok
ppp ipv6cp 0 0 0 0 ok
ppp mplscp 0 0 0 0 ok
ppp isis 0 0 0 0 ok
pppoe aggregate 61561238 0 4000 0 ok
pppoe padi 30780619 23086506 2000 1 viol
pppoe pado 0 0 0 0 ok
pppoe padr 30780619 23086499 2000 1 viol
pppoe pads 0 0 0 0 ok
pppoe padt 0 0 0 0 ok
pppoe padm 0 0 0 0 ok
pppoe padn 0 0 0 0 ok
dhcipv4 aggregate 0 0 0 0 ok
dhcipv4 unclass.. 0 0 0 0 ok
dhcipv4 discover 0 0 0 0 ok
dhcipv4 offer 0 0 0 0 ok
dhcipv4 request 0 0 0 0 ok
dhcipv4 decline 0 0 0 0 ok
dhcipv4 ack 0 0 0 0 ok
dhcipv4 nak 0 0 0 0 ok
dhcipv4 release 0 0 0 0 ok
dhcipv4 inform 0 0 0 0 ok
dhcipv4 renew 0 0 0 0 ok
dhcipv4 forcerenew 0 0 0 0 ok
dhcipv4 leasequery 0 0 0 0 ok
dhcipv4 leaseuna.. 0 0 0 0 ok
dhcipv4 leaseunk.. 0 0 0 0 ok
dhcipv4 leaseact.. 0 0 0 0 ok
dhcipv4 bootp 0 0 0 0 ok
dhcipv4 no-msgtype 0 0 0 0 ok
dhcipv4 bad-pack.. 0 0 0 0 ok

...

icmp aggregate 0 0 0 0 ok
igmp aggregate 0 0 0 0 ok
ospf aggregate 0 0 0 0 ok
rsvp aggregate 0 0 0 0 ok
pim aggregate 0 0 0 0 ok
rip aggregate 0 0 0 0 ok
ptp aggregate 0 0 0 0 ok
bfd aggregate 0 0 0 0 ok
lmp aggregate 0 0 0 0 ok
ldp aggregate 0 0 0 0 ok
msdp aggregate 0 0 0 0 ok
bgp aggregate 0 0 0 0 ok
vrrp aggregate 0 0 0 0 ok
telnet aggregate 0 0 0 0 ok

...

```

### show ddos-protection protocols statistics terse

```
user@host> show ddos-protection protocols statistics terse
```

| Protocol group | Packet type | Received (packets) | Dropped (packets) | Rate (pps) | Violation counts | State |
|----------------|-------------|--------------------|-------------------|------------|------------------|-------|
| ipv4-unc       | aggregate   | 241                | 0                 | 0          | 0                | ok    |
| icmp           | aggregate   | 20                 | 0                 | 0          | 0                | ok    |
| igmp           | aggregate   | 55                 | 0                 | 0          | 0                | ok    |
| ospf           | aggregate   | 956                | 0                 | 0          | 0                | ok    |
| rsvp           | aggregate   | 784                | 0                 | 0          | 0                | ok    |
| ldp            | aggregate   | 2984               | 0                 | 0          | 0                | ok    |
| bgp            | aggregate   | 312                | 0                 | 0          | 0                | ok    |
| lacp           | aggregate   | 1744               | 0                 | 0          | 0                | ok    |
| stp            | aggregate   | 9791               | 0                 | 0          | 0                | ok    |
| arp            | aggregate   | 19                 | 0                 | 0          | 0                | ok    |
| pvstp          | aggregate   | 393                | 0                 | 0          | 0                | ok    |
| mlp            | aggregate   | 624774             | 0                 | 0          | 0                | ok    |
| mlp            | packets     | 1714371            | 223937            | 0          | 3                | ok    |
| mcast-copy     | aggregate   | 3018038            | 0                 | 0          | 0                | ok    |
| igmp-snoop     | aggregate   | 43                 | 0                 | 0          | 0                | ok    |
| fw-host        | aggregate   | 95547              | 0                 | 0          | 0                | ok    |
| unc            | aggregate   | 10000              | 0                 | 0          | 0                | ok    |

### show ddos-protection protocols pppoe statistics

user@host> show ddos-protection protocols pppoe statistics

Protocol Group: PPPoE

Packet type: aggregate

System-wide information:

Aggregate bandwidth is never violated

Received: 60381200 Arrival rate: 4000 pps

Dropped: 0 Max arrival rate: 4002 pps

Routing Engine information:

Aggregate policer is never violated

Received: 15095242 Arrival rate: 1001 pps

Dropped: 0 Max arrival rate: 1011 pps

Dropped by individual policers: 0

FPC slot 1 information:

Aggregate policer is never violated

Received: 60381200 Arrival rate: 4000 pps

Dropped: 45287921 Max arrival rate: 4002 pps

Dropped by individual policers: 45287921

Packet type: padi

System-wide information:

Bandwidth is being violated!

No. of FPCs currently receiving excess traffic: 1

No. of FPCs that have received excess traffic: 1

Violation first detected at: 2011-04-19 08:23:17 PDT

Violation last seen at: 2011-04-19 12:34:48 PDT

Duration of violation: 04:11:31 Number of violations: 1

Received: 30190600 Arrival rate: 2000 pps

Dropped: 22643960 Max arrival rate: 2001 pps

Routing Engine information:

Policer is never violated

Received: 7547621 Arrival rate: 499 pps

Dropped: 0 Max arrival rate: 505 pps

Dropped by aggregate policer: 0

FPC slot 1 information:

Policer is currently being violated!

Violation first detected at: 2011-04-19 08:23:17 PDT

Violation last seen at: 2011-04-19 12:34:48 PDT

Duration of violation: 04:11:31 Number of violations: 1

```

Received: 30190600 Arrival rate: 2000 pps
Dropped: 22643960 Max arrival rate: 2001 pps
Dropped by this policer: 22643960
Dropped by aggregate policer: 0

```

Packet type: pado

System-wide information:

Bandwidth is never violated

```

Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps

```

Routing Engine information:

Policer is never violated

```

Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by aggregate policer: 0

```

FPC slot 1 information:

Policer is never violated

```

Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by aggregate policer: 0

```

Packet type: padr

System-wide information:

Bandwidth is being violated!

```

No. of FPCs currently receiving excess traffic: 1
No. of FPCs that have received excess traffic: 1
Violation first detected at: 2011-04-19 08:23:17 PDT
Violation last seen at: 2011-04-19 12:34:48 PDT
Duration of violation: 04:11:31 Number of violations: 1
Received: 30190600 Arrival rate: 2000 pps
Dropped: 22643961 Max arrival rate: 2001 pps

```

Routing Engine information:

Policer is never violated

```

Received: 7547621 Arrival rate: 501 pps
Dropped: 0 Max arrival rate: 506 pps
Dropped by aggregate policer: 0

```

FPC slot 1 information:

Policer is currently being violated!

```

Violation first detected at: 2011-04-19 08:23:17 PDT
Violation last seen at: 2011-04-19 12:34:48 PDT
Duration of violation: 04:11:31 Number of violations: 1
Received: 30190600 Arrival rate: 2000 pps
Dropped: 22643961 Max arrival rate: 2001 pps
Dropped by this policer: 22643961
Dropped by aggregate policer: 0

```

Packet type: pads

System-wide information:

Bandwidth is never violated

```

Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps

```

Routing Engine information:

Policer is never violated

```

Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by aggregate policer: 0

```

FPC slot 1 information:

Policer is never violated

```

Received: 0 Arrival rate: 0 pps
Dropped: 0 Max arrival rate: 0 pps
Dropped by aggregate policer: 0

```

```

Packet type: padt
System-wide information:
 Bandwidth is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
Routing Engine information:
 Policer is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
 Dropped by aggregate policer: 0
FPC slot 1 information:
 Policer is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
 Dropped by aggregate policer: 0

```

```

Packet type: padm
System-wide information:
 Bandwidth is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
:
 Policer is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
 Dropped by aggregate policer: 0
FPC slot 1 information:
 Policer is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
 Dropped by aggregate policer: 0

```

```

Packet type: padn
System-wide information:
 Bandwidth is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
:
 Policer is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
 Dropped by aggregate policer: 0
FPC slot 1 information:
 Policer is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
 Dropped by aggregate policer: 0

```

#### show ddos-protection protocols pppoe statistics brief

```

user@host> show ddos-protection protocols pppoe statistics brief

```

| Protocol | Packet    | Received  | Dropped   | Rate  | Violation | State |
|----------|-----------|-----------|-----------|-------|-----------|-------|
| group    | type      | (packets) | (packets) | (pps) | counts    |       |
| pppoe    | aggregate | 60901227  | 0         | 4000  | 0         | ok    |
| pppoe    | padi      | 30450613  | 22838981  | 2000  | 1         | viol  |
| pppoe    | pado      | 0         | 0         | 0     | 0         | ok    |
| pppoe    | padr      | 30450614  | 22838977  | 2000  | 1         | viol  |
| pppoe    | pads      | 0         | 0         | 0     | 0         | ok    |
| pppoe    | padt      | 0         | 0         | 0     | 0         | ok    |

|       |      |   |   |   |   |    |
|-------|------|---|---|---|---|----|
| pppoe | padm | 0 | 0 | 0 | 0 | ok |
| pppoe | padn | 0 | 0 | 0 | 0 | ok |

## show ddos-protection statistics

|                                 |                                                                                                                                                                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show ddos-protection statistics</b>                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.2.<br>Command introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.                                                                                                                                  |
| <b>Description</b>              | Display DDoS protection global statistics for bandwidth violations.                                                                                                                                                                                       |
| <b>Options</b>                  | This command has no options.                                                                                                                                                                                                                              |
| <b>Required Privilege Level</b> | view                                                                                                                                                                                                                                                      |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">clear ddos-protection protocols on page 318</a></li> <li>• <a href="#">show ddos-protection protocols on page 320</a></li> <li>• <a href="#">show ddos-protection version on page 355</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection statistics on page 354</a>                                                                                                                                                                                               |
| <b>Output Fields</b>            | <a href="#">Table 29 on page 354</a> lists the output fields for the <b>show ddos-protection statistics</b> command. Output fields are listed in the approximate order in which they appear.                                                              |

**Table 29: show ddos-protection statistics Output Fields**

| Field Name                        | Field Description                                                                                 |
|-----------------------------------|---------------------------------------------------------------------------------------------------|
| Currently violated packet types   | Number of packet types currently experiencing a bandwidth violation.                              |
| Packet types have seen violations | Number of packet types that have experienced a bandwidth violation since statistics were cleared. |
| Total violation counts            | Total number of bandwidth violations.                                                             |

## Sample Output

### show ddos-protection statistics

```

user@host> show ddos-protection statistics
DDOS protection global statistics:
 Currently violated packet types: 2
 Packet types have seen violations: 2
 Total violation counts: 2

```



## show ddos-protection version

**Syntax** `show ddos-protection version`

**Release Information** Command introduced in Junos OS Release 11.2.  
Command introduced in Junos OS Release 14.1X53-D40 for QFX5100 switches.

**Description** Display the DDoS protection version and the total numbers of protocol groups and packet types that can be configured in this version.



**NOTE:** Packet-type policers are not supported on QFX5100 switches.

**Options** This command has no options.

**Required Privilege Level** view

**Related Documentation**

- [clear ddos-protection protocols on page 318](#)
- [show ddos-protection protocols on page 320](#)
- [show ddos-protection statistics on page 354](#)

**List of Sample Output** [show ddos-protection version on page 355](#)

**Output Fields** [Table 30 on page 355](#) lists the output fields for the `show ddos-protection version` command. Output fields are listed in the approximate order in which they appear.

**Table 30: show ddos-protection version Output Fields**

| Field Name                 | Field Description                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Version                    | Version number of the DDoS protection code.                                                                                                  |
| Total protocol groups      | Number of protocol groups configured with DDoS protection.                                                                                   |
| Total tracked packet types | Number of protocol packet types configured with DDoS protection.<br><b>NOTE:</b> Packet-type policers are not supported on QFX5100 switches. |

## Sample Output

### show ddos-protection version

```
user@host> show ddos-protection version
DDoS protection, Version 1.0
 Total protocol groups = 83
 Total tracked packet types = 154
```

