

Security Feature Guide for QFX10000 Switches

Release
15.1



Modified: 2016-03-22

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 QFX10000 Switches

15.1

Copyright © 2016, Juniper Networks, Inc.

All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

	About the Documentation	xv
	Documentation and Release Notes	xv
	Supported Platforms	xv
	Using the Examples in This Manual	xv
	Merging a Full Example	xvi
	Merging a Snippet	xvi
	Documentation Conventions	xvii
	Documentation Feedback	xix
	Requesting Technical Support	xix
	Self-Help Online Tools and Resources	xix
	Opening a Case with JTAC	xx
Part 1	Firewall Filters	
Chapter 1	Configuring Firewall Filters	3
	Overview of Firewall Filters	3
	Firewall Filter Types	4
	Firewall Filter Components	5
	Firewall Filter Processing	5
	How Many Filters Are Supported?	5
	Understanding How Firewall Filters Are Evaluated	6
	Understanding How Firewall Filters Control Packet Flows	8
	Understanding Firewall Filter Match Conditions	9
	Filter Match Conditions	9
	Numeric Filter Match Conditions	9
	Interface Filter Match Conditions	10
	IP Address Filter Match Conditions	10
	MAC Address Filter Match Conditions	11
	Bit-Field Filter Match Conditions	11
	Firewall Filter Match Conditions and Actions for QFX10000 Switches	12
	Understanding How a Firewall Filter Tests a Protocol	23
	Understanding Firewall Filter Planning	24
	Planning the Number of Firewall Filters to Create	25
	Understanding How Many Firewall Filters Are Supported	25
	Egress Filters	27
	Avoid Configuring too Many Filters	27
	Policers can Limit Egress Filters	27
	Planning for Filter-Specific Policers	28

Understanding Firewall Filter Processing Points for Bridged and Routed	
Packets	29
Configuring Firewall Filters	30
Configuring a Firewall Filter	30
Applying a Firewall Filter to a Port	32
Applying a Firewall Filter to a VLAN	32
Applying a Firewall Filter to a Layer 3 (Routed) Interface	32
Applying Firewall Filters to Interfaces	33
Understanding Filter-Based Forwarding	34
Example: Using Filter-Based Forwarding to Route Application Traffic to a Security	
Device	34
Monitoring Firewall Filter Traffic	38
Monitoring Traffic for All Firewall Filters and Policers That Are	
Configured	38
Monitoring Traffic for a Specific Firewall Filter	39
Monitoring Traffic for a Specific Policer	39
Verifying That Firewall Filters Are Operational	39
Troubleshooting Firewall Filters	40
Troubleshooting QFX10000 Switches	40
Do Not Combine Match Conditions for Different Layers	40
Troubleshooting Other Switches	41
Firewall Filter Configuration Returns a No Space Available in TCAM	
Message	41
Filter Counts Previously Dropped Packet	42
Matching Packets Not Counted	43
Counter Reset When Editing Filter	44
Cannot Include loss-priority and policer Actions in Same Term	44
Cannot Egress Filter Certain Traffic Originating on QFX Switch	44
Firewall Filter Match Condition Not Working with Q-in-Q Tunneling	44
Egress Firewall Filters with Private VLANs	45
Egress Filtering of L2PT Traffic Not Supported	46
Cannot Drop BGP Packets in Certain Circumstances	46
Invalid Statistics for Policer	46
Policers can Limit Egress Filters	46

Part 2

Chapter 2

Policers

Configuring Policers	51
Overview of Policers	51
Policer Overview	52
Policer Types	52
Policer Actions	53
Policer Colors	54
Filter-Specific Policers	54
Suggested Naming Convention for Policers	55
Policer Counters	55
Policer Algorithms	55
How Many Policers Are Supported?	56

Policers Can Limit Egress Firewall Filters	56
Understanding Policers with Link Aggregation Groups	57
Understanding Color-Blind Mode for Single-Rate Tricolor Marking	57
Understanding Color-Aware Mode for Single-Rate Tricolor Marking	58
Summary of PLP Changes	58
Effect on Green Packets (Low PLP)	59
Effect on Yellow Packets (Medium PLP)	59
Effect on Red Packets (High PLP)	59
Understanding Color-Blind Mode for Two-Rate Tricolor Marking	60
Understanding Color-Aware Mode for Two-Rate Tricolor Marking	60
Summary of PLP Changes	60
Effect on Green Packets (Low PLP)	61
Effect on Yellow Packets (Medium PLP)	61
Effect on Red Packets (High PLP)	62
Example: Using Two-Color Policers and Prefix Lists	62
Example: Using Policers to Manage Oversubscription	65
Assigning Forwarding Classes and Loss Priority	67
Configuring Color-Blind Egress Policers for Medium-Low PLP	68
Configuring Two-Color and Three-Color Policers to Control Traffic Rates	69
Configuring Two-Color Policers	69
Configuring Three-Color Policers	70
Specifying Policers in a Firewall Filter Configuration	70
Applying a Firewall Filter That Includes a Policer	71
Verifying That Two-Color Policers Are Operational	71
Verifying That Three-Color Policers Are Operational	72
Troubleshooting Policer Configuration	72
Incomplete Count of Packet Drops	72
Counter Reset When Editing Filter	73
Invalid Statistics for Policer	73
Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured	73
Filter-Specific Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured	74
Policers Can Limit Egress Filters	75

Part 3

Configuring Port Security

Chapter 3

Port Security	79
Overview of Access Port Protection	79
Mitigation of Ethernet Switching Table Overflow Attacks	79
Mitigation of Rogue DHCP Server Attacks	80
Protection Against DHCP Starvation Attacks	80
Understanding MAC Limiting and MAC Move Limiting for Port Security	81
MAC Limiting	81
MAC Move Limiting	82
Actions for MAC Limiting	82

MAC Addresses That Exceed the MAC Limit or MAC Move Limit	82
Verifying That MAC Limiting Is Working Correctly	83
Verifying That MAC Limiting for Dynamic MAC Addresses Is Working Correctly	83
Verifying That Allowed MAC Addresses Are Working Correctly	84
Verifying That Interfaces Are Shut Down	84
Customizing the Ethernet Switching Table Display to View Information for a Specific Interface	85
Verifying That MAC Move Limiting Is Working Correctly	86
Verifying That the Port Error Disable Setting Is Working Correctly	86
Configuring Persistent MAC Learning (CLI Procedure)	87
Understanding Trusted and Untrusted Ports	89
Understanding Trusted DHCP Servers for Port Security	89
Verifying That a Trusted DHCP Server Is Working Correctly	89
Understanding DHCP Option 82 for Port Security	91
DHCP Option 82 Processing	91
Suboption Components of Option 82	92
Configurations That Support Option 82	92
Understanding Static ARP Entries	93

Part 4

Chapter 4

Configuring Device Security

Device Security	97
Understanding Storm Control	97
Example: Configuring Storm Control to Prevent Network Outages	98
Verifying That the Port Error Disable Setting Is Working Correctly	101
Understanding Unicast RPF	102
Unicast RPF for Switches Overview	102
Unicast RPF Implementation	103
Unicast RPF Packet Filtering	103
Bootstrap Protocol (BOOTP) and DHCP Requests	103
Default Route Handling	103
When to Enable Unicast RPF	103
When Not to Enable Unicast RPF	104
Limitations of the Unicast RPF Implementation on EX3200, EX4200, and EX4300 Switches	105
Configuring Unicast RPF (CLI Procedure)	106
Disabling Unicast RPF (CLI Procedure)	107
Verifying Unicast RPF Status	108
Understanding Unknown Unicast Forwarding	111
Configuring Unknown Unicast Forwarding (CLI Procedure)	111
Configuring Unknown Unicast Forwarding on EX4300 Switches	112
Configuring Unknown Unicast Forwarding on EX9200 Switches	112

Part 5	DDoS Protection	
Chapter 5	Overview of DDoS Protection	117
	Understanding Distributed Denial-of-Service Protection on QFX Series	
	Switches	117
	Policer Types and Packet Priorities	118
	Example of Policer Priority Behavior	118
	Policer Enforcement Points on QFX Series Switches	119
Chapter 6	Configuring DDoS Protection	121
	Configuring Protection Against DDoS Attacks	121
	Example: Configuring DDoS Protection on QFX Series Switches	122
	Disabling DDoS Protection Policers and Logging Globally	126
	Configuring DDoS Protection Policers on QFX Series Switches	126
	Configuring the Aggregate Policer for a Protocol Group	127
	Configuring Packet-Type Policers for a Protocol Group	128
	Configuring Policers on Individual Line Cards	129
	Disabling Policers and Policer Logging	129
	Tracing DDoS Protection Operations	130
	Configuring the DDoS Protection Trace Log Filename	131
	Configuring the Number and Size of DDoS Protection Log Files	131
	Configuring Access to the DDoS Protection Log File	132
	Configuring a Regular Expression for DDoS Protection Messages to Be	
	Logged	132
	Configuring the DDoS Protection Tracing Flags	132
	Configuring the Severity Level to Filter Which DDoS Protection Messages	
	Are Logged	133
Chapter 7	Monitoring DDoS Protection	135
	Verifying and Managing DDoS Protection	135
Part 6	Configuration Statements and Operational Commands	
Chapter 8	Configuration Statements (Firewall Filters)	139
	family	140
	filter	141
	filter (Layer 2 and Layer 3 Interfaces)	142
	filter (VLANs)	143
	firewall	144
	from	145
	input (Forwarding Table)	146
	interface-specific	146
	output (Forwarding Table)	147
	term	148
	then (Filters)	149
Chapter 9	Configuration Statements (Policers)	151
	action	152
	bandwidth-limit	152
	burst-size-limit	153
	color-aware	154

	color-blind	155
	committed-burst-size	156
	committed-information-rate	157
	excess-burst-size	158
	filter-specific	159
	firewall	160
	if-exceeding	161
	loss-priority high then discard (Three-Color Policer)	162
	peak-burst-size	163
	peak-information-rate	164
	policer	165
	single-rate	166
	then (Policers)	167
	three-color-policer	168
	two-rate	169
Chapter 10	Configuration Statements (Device Security)	171
	action-shutdown	172
	bandwidth-level	173
	bandwidth-percentage	174
	interface (Unknown Unicast Forwarding)	175
	no-broadcast	176
	no-multicast	177
	no-unknown-unicast	178
	rpf-check	179
	storm-control	180
	storm-control-profiles	181
	unknown-unicast-forwarding	182
Chapter 11	Configuration Statements (Port Security)	183
	circuit-id	184
	fc-map	186
	fcoe-trusted	188
	mac-move-limit	189
	no-allowed-mac-log	190
	no-gratuitous-arp-request	191
	persistent-learning	191
	port-error-disable	192
	vendor-id	194
	write-interval	195
Chapter 12	Configuration Statements (DDoS Protection)	197
	bandwidth (DDoS)	198
	bandwidth-scale (DDoS)	199
	burst (DDoS)	200
	burst-scale (DDoS)	201
	bypass-aggregate (DDoS)	202
	ddos-protection (DDoS)	203
	disable-fpc (DDoS)	204
	disable-logging (DDoS)	205

	fpc (DDoS)	206
	global (DDoS)	207
	priority (DDoS)	208
	protocols (DDoS)	209
	traceoptions (DDoS)	214
Chapter 13	Operational Commands (Firewall Filters)	217
	clear firewall	218
	show firewall	219
	show firewall policer	223
	show interfaces filters	225
	show pfe filter hw summary	227
Chapter 14	Operational Commands (Port Security)	229
	clear ethernet-switching port-error	230
Chapter 15	Operational Commands (DDos Protection)	231
	clear ddos-protection protocols	232
	show ddos-protection protocols	234
	show ddos-protection protocols parameters	253
	show ddos-protection protocols statistics	260
	show ddos-protection statistics	270
	show ddos-protection version	272
	show ddos-protection protocols violations	273

List of Figures

Part 1	Firewall Filters	
Chapter 1	Configuring Firewall Filters	3
	Figure 1: Evaluation of Terms Within a Firewall Filter	7
	Figure 2: Application of Firewall Filters to Control Packet Flow	8
Part 2	Policers	
Chapter 2	Configuring Policers	51
	Figure 3: Flow of Tricolor Marking Policer Operation	52
Part 3	Configuring Port Security	
Chapter 3	Port Security	79
	Figure 4: Switch Relays DHCP Requests to Server	93
Part 4	Configuring Device Security	
Chapter 4	Device Security	97
	Figure 5: Symmetrically Routed Interfaces	104
	Figure 6: Asymmetrically Routed Interfaces	105

List of Tables

	About the Documentation	xv
	Table 1: Notice Icons	xvii
	Table 2: Text and Syntax Conventions	xvii
Part 1	Firewall Filters	
Chapter 1	Configuring Firewall Filters	3
	Table 3: Supported Firewall Filter Numbers for Specific Switches	5
	Table 4: Actions for Firewall Filters	12
	Table 5: Supported Match Conditions for Firewall Filters on QFX10000 Switches	13
	Table 6: Actions for Firewall Filters on QFX10000 Switches	21
	Table 7: Action Modifiers for Firewall Filters on QFX10000 Switches	21
	Table 8: Supported Firewall Filter Numbers	26
Part 2	Policers	
Chapter 2	Configuring Policers	51
	Table 9: Policer Actions	53
	Table 10: Color-Blind Mode TCM Color-to-PLP Mapping	58
	Table 11: Color-Aware Mode Single-Rate PLP Mapping	58
	Table 12: Color-Blind Mode TCM Color-to-PLP Mapping	60
	Table 13: Color-Aware Mode Two-Rate PLP Mapping	60
	Table 14: Servers Connected to Switch	65
	Table 15: Unicast Forwarding Classes	67
Part 6	Configuration Statements and Operational Commands	
Chapter 12	Configuration Statements (DDoS Protection)	197
	Table 16: Packet Types Supported by DDoS Protection on QFX Switches	209
	Table 17: Protocol Groups Supported by DDoS Protection on QFX Switches	211
Chapter 13	Operational Commands (Firewall Filters)	217
	Table 18: show firewall Output Fields	219
	Table 19: show firewall policer Output Fields	223
	Table 20: show interfaces filters Output Fields	225
	Table 21: show pfe filter hw summary Output Fields	227
Chapter 15	Operational Commands (DDoS Protection)	231
	Table 22: Supported Protocol Groups	238
	Table 23: show ddos-protection protocols Output Fields	244
	Table 24: show ddos-protection protocols parameters Output Fields	254

Table 25: show ddos-protection protocols statistics Output Fields	261
Table 26: show ddos-protection statistics Output Fields	270
Table 27: show ddos-protection version Output Fields	272
Table 28: show ddos-protection protocols violations Output Fields	273

About the Documentation

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

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 the *CLI User Guide*.

Documentation Conventions

Table 1 on page xvii 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 xvii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

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

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

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric metric>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (string1 string2 string3)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<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

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

CHAPTER 1

Configuring Firewall Filters

- Overview of Firewall Filters on page 3
- Understanding How Firewall Filters Are Evaluated on page 6
- Understanding How Firewall Filters Control Packet Flows on page 8
- Understanding Firewall Filter Match Conditions on page 9
- Firewall Filter Match Conditions and Actions for QFX10000 Switches on page 12
- Understanding How a Firewall Filter Tests a Protocol on page 23
- Understanding Firewall Filter Planning on page 24
- Planning the Number of Firewall Filters to Create on page 25
- Understanding Firewall Filter Processing Points for Bridged and Routed Packets on page 29
- Configuring Firewall Filters on page 30
- Applying Firewall Filters to Interfaces on page 33
- Understanding Filter-Based Forwarding on page 34
- Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on page 34
- Monitoring Firewall Filter Traffic on page 38
- Verifying That Firewall Filters Are Operational on page 39
- Troubleshooting Firewall Filters on page 40

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](#)
- [How Many Filters Are Supported? 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.

How Many Filters Are Supported?

QFX10000 switches support 8K firewall filters and 64K firewall filter terms.

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 3 on page 5](#).

Table 3: Supported Firewall Filter Numbers for Specific Switches

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. The actual number of filters that these

switches will support depends on how the filters are stored in ternary content addressable memory (TCAM). See [“Planning the Number of Firewall Filters to Create” on page 25](#) for detailed information about this topic.

**Related
Documentation**

- [Understanding Firewall Filter Planning on page 24](#)
- [Understanding Firewall Filter Processing Points for Bridged and Routed Packets on page 29](#)
- [Understanding How Firewall Filters Are Evaluated on page 6](#)
- [Understanding Firewall Filter Match Conditions on page 9](#)
- [Overview of Policers on page 51](#)
- [Configuring Firewall Filters on page 30](#)

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.

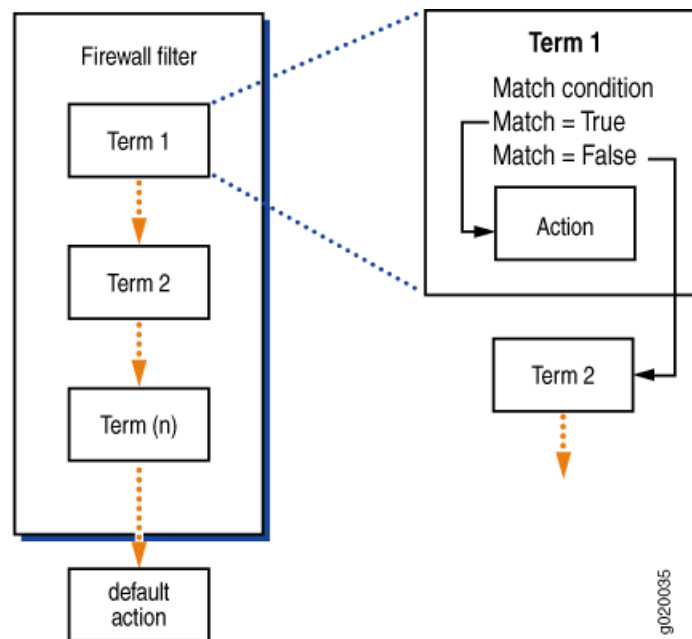
4. If a packet passes through all the terms in the filter without a match, the switch discards it.



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 7](#) 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 9](#)
- [Overview of Policers on page 51](#)
- [Configuring Firewall Filters on page 30](#)

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).

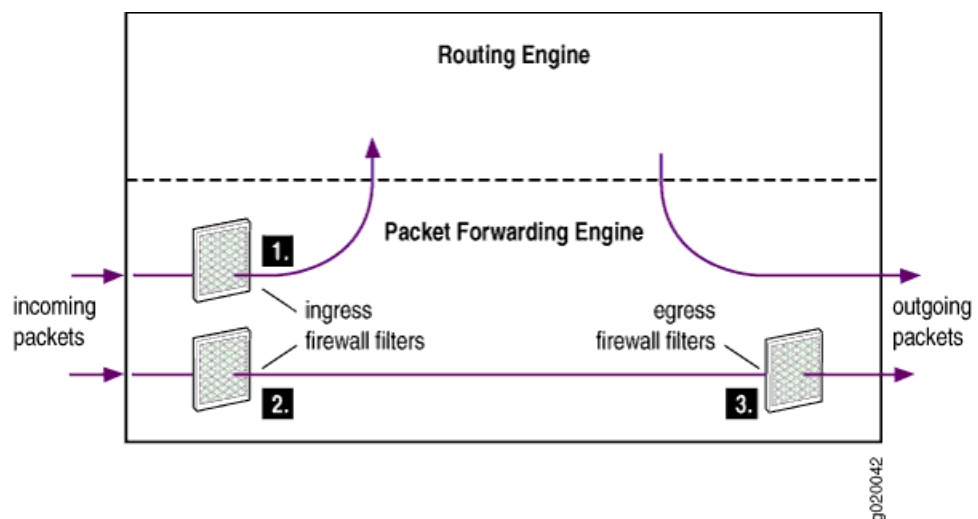
Firewall filters affect packet flows entering into or exiting from a switch as follows:

- 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 8 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 29](#)
- [Understanding How Firewall Filters Are Evaluated on page 6](#)
- [Configuring Firewall Filters on page 30](#)

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 9](#)
- [Numeric Filter Match Conditions on page 9](#)
- [Interface Filter Match Conditions on page 10](#)
- [IP Address Filter Match Conditions on page 10](#)
- [MAC Address Filter Match Conditions on page 11](#)
- [Bit-Field Filter Match Conditions on page 11](#)

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 (0) 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/*/6.0
user@switch# set interface ge-0/1/*0
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 4 on page 12](#). The operators are listed in order from highest precedence to lowest precedence. Operations are evaluated from left to right.

Table 4: 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 23](#)
- [Firewall Filter Match Conditions and Actions](#)
- [Configuring Firewall Filters on page 30](#)

Firewall Filter Match Conditions and Actions for QFX10000 Switches

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 firewall filters on QFX10000 switches. For similar information about other QFX switches, see *Firewall Filter Match Conditions and Actions*.

- [Table 5 on page 13](#) 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 6 on page 21](#) shows the actions that you can specify in a term.
- [Table 7 on page 21](#) shows the action modifiers you can use to count, mirror, rate-limit, and classify packets.



NOTE: On QFX10000 switches, do not combine match conditions for Layer 2 and any other layer in a family ethernet-switching filter. (For example, do not include conditions that match MAC addresses and IP addresses in the same filter.) If you do so, the filter will commit successfully but will not work. You will also see the following log message: **L2 filter *filter-name* doesn't support mixed L2 and L3/L4 match conditions. Please re-config.**

Table 5: Supported Match Conditions for Firewall Filters on QFX10000 Switches

Match Condition	Description	Direction and Interface
destination-address <i>ip-address</i>	IP destination address field, which is the address of the final destination node.	Ingress Pv4 (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 and VLANs. Egress ports and VLANs.

Table 5: Supported Match Conditions for Firewall Filters on QFX10000 Switches (*continued*)

Match Condition	Description	Direction and Interface
destination-port <i>value</i>	<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>xdmcp (177),</p> <p>zephyr-clt (2103), zephyr-hm (2104)</p>	<p>Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p> <p>Egress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p>
destination-prefix-list <i>prefix-list</i>	<p>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.</p>	<p>Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p> <p>Egress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p>

Table 5: Supported Match Conditions for Firewall Filters on QFX10000 Switches (*continued*)

Match Condition	Description	Direction and Interface
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 	<p>Ingress ports, VLANs, and IPv4 (inet) interfaces.</p> <p>Egress ports, VLANs, and IPv4 (inet) interfaces.</p>
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>

Table 5: Supported Match Conditions for Firewall Filters on QFX10000 Switches (*continued*)

Match Condition	Description	Direction and Interface
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, VLANs, and IPv4 (inet) interfaces.
hop-limit value	Match 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.
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 ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces</p>

Table 5: Supported Match Conditions for Firewall Filters on QFX10000 Switches (*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 ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) 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, egress ports, and VLANs.
ip-options	Specify any to create a match if anything is specified in the options field in the IP header.	Ingress ports, VLANs, and IPv4 (inet) interfaces.
ip-precedence ip-precedence-field	<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 and VLANs.</p> <p>Egress ports and VLANs.</p>
ip-protocol <i>number</i>	IP protocol field.	<p>Ingress ports and VLANs.</p> <p>Egress ports and VLANs.</p>

Table 5: Supported Match Conditions for Firewall Filters on QFX10000 Switches (*continued*)

Match Condition	Description	Direction and Interface
ip-source-address <i>address</i>	IPv4 address of the source node sending the packet.	Ingress ports and VLANs. Egress ports and VLANs.
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. Egress 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.
learn-ip-priority <i>number</i>	Matches the specified IEEE 802.1p VLAN priority bits in the range 0-7.	Ingress ports and VLANs. Egress ports and VLANs.
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). To use filter memory most efficiently and maximize the number of possible filters, use this condition in addition to user-id when you want to match on the inner (customer) VLAN ID. The acceptable values are 1-4095.	Ingress ports and VLANs. Egress ports and VLANs.
next-header <i>value</i>	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 IPv6 (inet6) interfaces. Egress IPv6 (inet6) interfaces.
packet-length <i>number</i>	Packet length in bytes. You must enter a number between 0 and 65535.	Ingress ports, VLANs, IPv4 (inet), and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.

Table 5: Supported Match Conditions for Firewall Filters on QFX10000 Switches (*continued*)

Match Condition	Description	Direction and Interface
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 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 IPv4 (inet) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>
source-address ip-address	IP source address field, which is the address of the node that sent the packet.	<p>Ingress IPv4 (inet) interfaces and IPv6 (inet6) interfaces.</p> <p>Egress IPv4 (inet) interfaces and IPv6 (inet6) 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 ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p>
source-prefix-list <i>prefix-list</i>	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.	<p>Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p> <p>Egress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.</p>

Table 5: Supported Match Conditions for Firewall Filters on QFX10000 Switches (*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>
traffic-class value	<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 IPv6 (inet6) interfaces.</p> <p>Egress IPv6 (inet6) interfaces.</p>
ttl value	<p>IP Time-to-live (TTL) field in decimal. The value can be 1–255.</p>	<p>Ingress IPv4 (inet) interfaces.</p> <p>Egress IPv4 (inet) interfaces.</p>
user-vlan-id number	<p>Matches the ID of the inner (customer) VLAN in a Q-in-Q VLAN. To use filter memory most efficiently and maximize the number of possible filters, use in combination with learn-vlan-id to match the outer (service) VLAN ID. The acceptable values are 1–4095.</p>	<p>Ingress ports and VLANs.</p> <p>Egress ports and VLANs.</p>

Use **then** statements to define actions that should occur if a packet matches all conditions in a **from** statement. [Table 6 on page 21](#) 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 6: Actions for Firewall Filters on QFX10000 Switches

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.
reject message-type	<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 instance-name	Forward matched packets to a virtual routing instance. (The only supported instance type is virtual-router .) Packets can be forwarded to the default instance.
vlan VLAN-name	<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 7 on page 21](#) to count, mirror, rate-limit, and classify packets.

Table 7: Action Modifiers for Firewall Filters on QFX10000 Switches

Action Modifier	Description
count counter-name	Count the number of packets that match the term.

Table 7: Action Modifiers for Firewall Filters on QFX10000 Switches (*continued*)

Action Modifier	Description
forwarding-class <i>class</i>	<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>
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 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>
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 and egress port, VLAN, IPv4 (inet), and IPv6 (inet6) firewall 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 and egress port, VLAN, IPv4 (inet), and IPv6 (inet6) firewall filters.</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 and egress port, VLAN, IPv4 (inet), and IPv6 (inet6) firewall filters.</p> <p>NOTE:</p>
syslog	<p>Log an alert for this packet.</p> <p>NOTE: The syslog action modifier is supported on ingress interfaces only.</p>

Table 7: Action Modifiers for Firewall Filters on QFX10000 Switches (*continued*)

Action Modifier	Description
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), and IPv6 (inet6) 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 6](#)
 - [Understanding How a Firewall Filter Tests a Protocol on page 23](#)
 - [Overview of Policers on page 51](#)
 - [Understanding Port Mirroring](#)
 - [Configuring Firewall Filters on page 30](#)

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 9](#)
 - [Configuring Firewall Filters on page 30](#)

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 25 for information about how many firewall filters you can apply.

Related Documentation

- [Overview of Policers on page 51](#)
- [Understanding How Firewall Filters Are Evaluated on page 6](#)
- [Configuring Firewall Filters on page 30](#)

Planning the Number of Firewall Filters to Create

- [Understanding How Many Firewall Filters Are Supported on page 25](#)
- [Egress Filters on page 27](#)
- [Avoid Configuring too Many Filters on page 27](#)
- [Policers can Limit Egress Filters on page 27](#)
- [Planning for Filter-Specific Policers on page 28](#)

Understanding How Many Firewall Filters Are Supported

QFX10000 switches support 8K firewall filters and 64K firewall filter terms.

QFX3500, QFX3600, QFX5100, and EX4600 switches, QFabric Node devices, and VCF members store firewall filters in ternary content addressable memory (TCAM) and support the maximum numbers of firewall filter terms per type of attachment point shown in [Table 8 on page 26](#). (QFX10000 switches do not use TCAM.)

Table 8: 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 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, 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. 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.

Policers can Limit Egress Filters

On some switches, the number of egress policers that you configure can affect the total number of allowed egress firewall filters. (This issue does not affect QFX10000 switches.) On the affected switches, 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.

**Related
Documentation**

- [Understanding How Firewall Filters Are Evaluated on page 6](#)
- [Understanding Firewall Filter Planning on page 24](#)
- [Configuring Firewall Filters on page 30](#)
- [Understanding Filter-Based Forwarding on page 34](#)

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 8](#)
- [Configuring Firewall Filters on page 30](#)

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 30](#)
- [Applying a Firewall Filter to a Port on page 32](#)
- [Applying a Firewall Filter to a VLAN on page 32](#)
- [Applying a Firewall Filter to a Layer 3 \(Routed\) Interface on page 32](#)

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](#)
- [Verifying That Firewall Filters Are Operational on page 39](#)
- [Monitoring Firewall Filter Traffic on page 38](#)
- [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 30](#)

Understanding 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.

You might want to use filter-based forwarding to route specific types of traffic through a firewall or other security device before the traffic continues on its path. You can also use filter-based forwarding to give certain types of traffic preferential treatment. For example, you might want to ensure that the highest-priority traffic is forwarded over a 40-Gigabit Ethernet link. You might also use filter-based forwarding to obtain more control over load balancing than dynamic routing protocols provide.



NOTE: You can create as many as 128 filters or terms that direct packets to a given virtual routing instance.

Related Documentation

- [Understanding Virtual Router Routing Instances](#)
- [Overview of Firewall Filters on page 3](#)
- [Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on page 34](#)

Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device

You can configure filter-based forwarding by using a firewall filter to forward matched traffic to a specific virtual routing instance.

This example describes how to set up filter-based forwarding:

- [Requirements on page 35](#)
- [Overview and Topology on page 35](#)
- [Configuration on page 35](#)
- [Verification on page 37](#)

Requirements

This example requires Junos OS Release 15.1X53-D10 or later on a QFX10000 switch..

Overview and Topology

In this example, traffic from one application server that is destined for a different application server is matched by a firewall filter based on the IP address of the source application server. Any matching packets are routed to a virtual routing instance that sends the traffic to a security device. In this case, the security device must be able to forward the traffic to the destination application server. For this example, assume that the address of the destination application server is 192.168.0.1.



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

Configuration

To configure filter-based forwarding:

CLI Quick Configuration

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

```
[edit]
set interfaces xe-0/0/0 unit 0 family inet address 10.1.0.1/24
set interfaces xe-0/0/3 unit 0 family inet address 10.1.3.1/24
set firewall family inet filter f1 term t1 from source-address 10.1.0.50/32
set firewall family inet filter f1 term t1 from protocol tcp
set interfaces xe-0/0/0 unit 0 family inet filter input f1
set routing-instances vrf01 instance-type virtual-router
set routing-instances vrf01 interface xe-0/0/3.0
set routing-instances vrf01 routing-options static route 192.168.0.1/24 next-hop 10.1.3.254
set firewall family inet filter f1 term t1 then routing-instance vrf01
```

Step-by-Step Procedure

To configure filter-based forwarding:

1. Configure an interface to connect to the application server:


```
[edit interfaces]
user@switch# set xe-0/0/0 unit 0 family inet address 10.1.0.1/24
```
2. Configure an interface to connect to the security device:


```
[edit interfaces]
user@switch# set xe-0/0/3 unit 0 family inet address 10.1.3.1/24
```
3. Create a firewall filter that matches packets based on the address of the application server that the traffic will be sent from. Also configure the filter so that it matches only TCP packets:


```
[edit firewall]
user@switch# set family inet filter f1 term t1 from source-address 10.1.0.50/32
user@switch# set firewall family inet filter f1 term t1 from protocol tcp
```
4. Apply the filter to the interface that connects to the source application server and configure it to match incoming packets:

- ```
[edit interfaces]
user@switch# set xe-0/0/0 unit 0 family inet filter input f1
```
5. Create a virtual router:
 

```
[edit]
user@switch# set routing-instances vrf01 instance-type virtual-router
```
  6. Associate the virtual router with the interface that connects to the security device:
 

```
[edit routing-instances]
user@switch# set vrf01 interface xe-0/0/3.0
```
  7. Configure the routing information for the virtual routing instance:
 

```
[edit routing-instances]
user@switch# set vrf01 routing-options static route 192.168.0.1/24 next-hop 10.1.3.254
```
  8. Set the filter to forward packets to the virtual router:
 

```
[edit firewall]
user@switch# set family inet filter f1 term t1 then routing-instance vrf01
```

## Results

Check the results of the configuration:

```
user@switch> show configuration
interfaces {
 xe-0/0/0 {
 unit 0 {
 family inet {
 filter {
 input f1;
 }
 address 10.1.0.1/24;
 }
 }
 }
 xe-0/0/3 {
 unit 0 {
 family inet {
 address 10.1.3.1/24;
 }
 }
 }
}
firewall {
 family inet {
 filter f1 {
 term t1 {
 from {
 source-address {
 10.1.0.50/32;
 }
 protocol tcp;
 }
 then {
 routing-instance vrf01;
 }
 }
 }
 }
}
```



```

 }
 }
 routing-instances {
 vrf01 {
 instance-type virtual-router;
 interface xe-0/0/1.0;
 routing-options {
 static {
 route 12.34.56.0/24 next-hop 10.1.3.254;
 }
 }
 }
 }
}

```

## Verification

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

- [Verifying That Filter-Based Forwarding Was Configured on page 37](#)

### Verifying That Filter-Based Forwarding Was Configured

**Purpose** Verify that filter-based forwarding was properly enabled on the switch.

**Action** 1. Use the `show interfaces filters` command:

```

user@switch> show interfaces filters xe-0/0/0.0
Interface Admin Link Proto Input Filter Output Filter
xe-0/0/0.0 up down inet f1

```

2. Use the `show route forwarding-table` command:

```

user@switch> show route forwarding-table

Routing table: default.inet
Internet:
Destination Type RtRef Next hop Type Index NhRef Netif
default user 1 0:12:f2:21:cf:0 ucst 331 4 me0.0
default perm 0 rjct 36 3
0.0.0.0/32 perm 0 dscd 34 1
10.1.0.0/24 ifdn 0 rslv 613 1 xe-0/0/0.0
10.1.0.0/32 iddn 0 10.1.0.0 recv 611 1 xe-0/0/0.0
10.1.0.1/32 user 0 rjct 36 3
10.1.0.1/32 intf 0 10.1.0.1 locl 612 2
10.1.0.1/32 iddn 0 10.1.0.1 locl 612 2
10.1.0.255/32 iddn 0 10.1.0.255 bcst 610 1 xe-0/0/0.0
10.1.1.0/26 ifdn 0 rslv 583 1 vlan.0
10.1.1.0/32 iddn 0 10.1.1.0 recv 581 1 vlan.0
10.1.1.1/32 user 0 rjct 36 3
10.1.1.1/32 intf 0 10.1.1.1 locl 582 2
10.1.1.1/32 iddn 0 10.1.1.1 locl 582 2
10.1.1.63/32 iddn 0 10.1.1.63 bcst 580 1 vlan.0
255.255.255.255/32 perm 0 bcst 32 1

```

```

Routing table: vrf01.inet
Internet:
Destination Type RtRef Next hop Type Index NhRef Netif
default perm 0 rjct 559 2
0.0.0.0/32 perm 0 dscd 545 1

```

```

10.1.3.0/24 ifdn 0 rslv 617 1 xe-0/0/3.0
10.1.3.0/32 iddn 0 10.1.3.0 recv 615 1 xe-0/0/3.0
10.1.3.1/32 user 0 rjct 559 2
192.168.0.1/24 user 0 10.1.3.254 ucst 616 2 xe-0/0/3.0
192.168.0.1/24 user 0 10.1.3.254 ucst 616 2 xe-0/0/3.0
10.1.3.255/32 iddn 0 10.1.3.255 bcst 614 1 xe-0/0/3.0
224.0.0.0/4 perm 0 mdsc 546 1
224.0.0.1/32 perm 0 224.0.0.1 mcst 529 1
255.255.255.255/32 perm 0 bcst 543 1

```

Routing table: default.iso

ISO:

| Destination | Type | RtRef | Next hop | Type | Index | NhRef | Netif |
|-------------|------|-------|----------|------|-------|-------|-------|
| default     | perm | 0     |          | rjct | 60    | 1     |       |

Routing table: vrf01.iso

ISO:

| Destination | Type | RtRef | Next hop | Type | Index | NhRef | Netif |
|-------------|------|-------|----------|------|-------|-------|-------|
| default     | perm | 0     |          | rjct | 600   | 1     |       |

**Meaning** The output indicates that the filter was created on the interface and that the virtual routing instance is forwarding matching traffic to the correct IP address.

- Related Documentation**
- [Configuring Firewall Filters on page 30](#)
  - [Understanding Filter-Based Forwarding on page 34](#)
  - [Understanding Virtual Router Routing Instances](#)

## 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 38](#)
- [Monitoring Traffic for a Specific Firewall Filter on page 39](#)
- [Monitoring Traffic for a Specific Policer on page 39](#)

### 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 30](#)
- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 69](#)
- [Verifying That Firewall Filters Are Operational on page 39](#)

### 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 30](#)
- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 69](#)
- [Monitoring Firewall Filter Traffic on page 38](#)

---

## Troubleshooting Firewall Filters

Use the following information to troubleshoot your firewall filter configuration.

- [Troubleshooting QFX10000 Switches on page 40](#)
- [Troubleshooting Other Switches on page 41](#)

## Troubleshooting QFX10000 Switches

This section describes an issue specific to QFX10000 switches:

- [Do Not Combine Match Conditions for Different Layers on page 40](#)

---

### Do Not Combine Match Conditions for Different Layers

On QFX10000 switches, do not combine match conditions for Layer 2 and any other layer in a **family ethernet-switching** filter. (For example, do not include conditions that match MAC addresses and IP addresses in the same filter.) If you do so, the filter will commit successfully but will not work. You will also see the following log message: **L2 filter *filter-name* doesn't support mixed L2 and L3/L4 match conditions. Please re-config.**

## Troubleshooting Other Switches

This section describes issues specific to QFX switches other than QFX10000 switches. This information also applies to OCX1100 switches and EX4600 switches.

- [Firewall Filter Configuration Returns a No Space Available in TCAM Message on page 41](#)
- [Filter Counts Previously Dropped Packet on page 42](#)
- [Matching Packets Not Counted on page 43](#)
- [Counter Reset When Editing Filter on page 44](#)
- [Cannot Include loss-priority and policer Actions in Same Term on page 44](#)
- [Cannot Egress Filter Certain Traffic Originating on QFX Switch on page 44](#)
- [Firewall Filter Match Condition Not Working with Q-in-Q Tunneling on page 44](#)
- [Egress Firewall Filters with Private VLANs on page 45](#)
- [Egress Filtering of L2PT Traffic Not Supported on page 46](#)
- [Cannot Drop BGP Packets in Certain Circumstances on page 46](#)
- [Invalid Statistics for Policer on page 46](#)
- [Policers can Limit Egress Filters on page 46](#)

### 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 **admin**VLAN, 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:** On some switches, the number of egress policers that you configure can affect the total number of allowed egress firewall filters. (This issue does not affect QFX10000 switches.) On the affected switches, 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 2

# Policers

- [Configuring Policers on page 51](#)



## CHAPTER 2

# Configuring Policers

- [Overview of Policers on page 51](#)
- [Understanding Policers with Link Aggregation Groups on page 57](#)
- [Understanding Color-Blind Mode for Single-Rate Tricolor Marking on page 57](#)
- [Understanding Color-Aware Mode for Single-Rate Tricolor Marking on page 58](#)
- [Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 60](#)
- [Understanding Color-Aware Mode for Two-Rate Tricolor Marking on page 60](#)
- [Example: Using Two-Color Policers and Prefix Lists on page 62](#)
- [Example: Using Policers to Manage Oversubscription on page 65](#)
- [Assigning Forwarding Classes and Loss Priority on page 67](#)
- [Configuring Color-Blind Egress Policers for Medium-Low PLP on page 68](#)
- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 69](#)
- [Verifying That Two-Color Policers Are Operational on page 71](#)
- [Verifying That Three-Color Policers Are Operational on page 72](#)
- [Troubleshooting Policer Configuration on page 72](#)

## 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 52](#)
- [Policer Types on page 52](#)
- [Policer Actions on page 53](#)
- [Policer Colors on page 54](#)
- [Filter-Specific Policers on page 54](#)
- [Suggested Naming Convention for Policers on page 55](#)
- [Policer Counters on page 55](#)
- [Policer Algorithms on page 55](#)

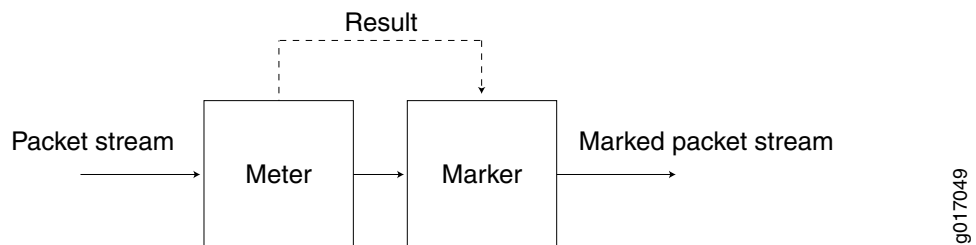
- [How Many Policers Are Supported? on page 56](#)
- [Policies Can Limit Egress Firewall Filters on page 56](#)

## 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 52](#) illustrates this process.

**Figure 3: Flow of Tricolor Marking Policer Operation**



After you name and configure a policer, you can 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 9 on page 53](#) 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 9 on page 53](#) describes the policer actions.

**Table 9: 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 9: 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 on some QFX switches, 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. (This behavior does not occur in QFX10000 switches.)

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 25](#) 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 ***policer#-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

On some QFX switches, 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 and provides the total amount. (This does not apply to QFX10000 switches.) If you want to obtain separate packet counts for each term on an affected switch, 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.



**NOTE:** In an environment of light bursty traffic, QFX5200 might not replicate all multicast packets to two or more downstream interfaces. This occurs only at a line rate burst—if traffic is consistent, the issue does not occur. In addition, the issue occurs only when packet size increases beyond 6k in a one gigabit traffic flow.

## How Many Policers Are Supported?

QFX10000 switches support 8K policers (all policer types). QFX5100 and QFX5200 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

On some switches, the number of egress policers that you configure can affect the total number of allowed egress firewall filters. (This issue does not affect QFX10000 switches.) On the affected switches, 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 57](#)
- [Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 60](#)
- [Understanding Color-Aware Mode for Single-Rate Tricolor Marking on page 58](#)
- [Understanding Color-Aware Mode for Two-Rate Tricolor Marking on page 60](#)
- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 69](#)

---

## 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 51](#)
- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 69](#)

---

## 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 10 on page 58](#).

Table 10: 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 51](#)
- [Configuring Color-Blind Egress Policers for Medium-Low PLP on page 68](#)

## 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 11 on page 58 shows how a packet's incoming priority can be modified with single-rate marking.

Table 11: 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 51](#)
  - [Configuring Color-Blind Egress Policers for Medium-Low PLP on page 68](#)

## 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 12: Color-Blind Mode TCM Color-to-PLP Mapping**

| Color  | PLP                | Meaning                                             |
|--------|--------------------|-----------------------------------------------------|
| Green  | <b>low</b>         | Packet does not exceed the CIR.                     |
| Yellow | <b>medium-high</b> | Packet exceeds the CIR but does not exceed the PIR. |
| Red    | <b>high</b>        | Packet exceeds the PIR.                             |

- Related Documentation**
- [Overview of Policers on page 51](#)
  - [Configuring Color-Blind Egress Policers for Medium-Low PLP on page 68](#)

## 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 13 on page 60](#) shows how a packet's incoming priority can be modified with two-rate marking.

**Table 13: Color-Aware Mode Two-Rate PLP Mapping**

| Incoming PLP      | Packet Metered Against | Possible Cases                          | Outgoing PLP       |
|-------------------|------------------------|-----------------------------------------|--------------------|
| <b>low</b>        | CIR and PIR            | Packet does not exceed the CIR.         | <b>low</b>         |
|                   |                        | Packet exceeds the CIR but not the PIR. | <b>medium-high</b> |
|                   |                        | Packet exceeds the PIR.                 | <b>high</b>        |
| <b>medium-low</b> | PIR only               | Packet does not exceed the PIR.         | <b>medium-low</b>  |
|                   |                        | Packet exceeds the PIR.                 | <b>high</b>        |



Table 13: Color-Aware Mode Two-Rate PLP Mapping (*continued*)

| Incoming PLP | Packet Metered Against      | Possible Cases                  | Outgoing PLP |
|--------------|-----------------------------|---------------------------------|--------------|
| 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 51](#)
- [Configuring Color-Blind Egress Policers for Medium-Low PLP on page 68](#)

---

## 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;
 }
 }
 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 51](#)
  - [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 14 on page 65](#).

**Table 14: 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 51](#)

## 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 15 on page 67](#)

**Table 15: 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 30](#). (Assigning forwarding classes and PLP is supported only on ingress filters.)

#### Related Documentation

- [Configuring Firewall Filters on page 30](#)
- [Verifying That Firewall Filters Are Operational on page 39](#)
- [Monitoring Firewall Filter Traffic on page 38](#)
- [Overview of Policers on page 51](#)
- [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 51](#)
- [Understanding Color-Blind Mode for Single-Rate Tricolor Marking on page 57](#)
- [Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 60](#)
- [Configuring Firewall Filters on page 30](#)
- [Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 69](#)

## 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 69](#)
2. [Configuring Three-Color Policers on page 70](#)
3. [Specifying Policers in a Firewall Filter Configuration on page 70](#)
4. [Applying a Firewall Filter That Includes a Policer on page 71](#)

### 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 Policar

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 30.



**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 30](#)
- [Overview of Policers on page 51](#)
- [Verifying That Two-Color Policers Are Operational on page 71](#)
- [Verifying That Three-Color Policers Are Operational on page 72](#)
- [Configuring Color-Blind Egress Policers for Medium-Low PLP on page 68](#)

## 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
icmp-connection-policer
tcp-connection-policer
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```

```
Packets
10
539
```

|                              |                                                                                                                                                                                                                                                                                                |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Meaning</b>               | The <b>show firewall policer</b> 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.     |
| <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 69</a></li><li>• <a href="#">Configuring Firewall Filters on page 30</a></li><li>• <a href="#">Monitoring Firewall Filter Traffic on page 38</a></li></ul> |

---

## Verifying That Three-Color Policers Are Operational

|                              |                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>               | Verify that three-color policers in firewall filter configurations are working properly.                                                                                                                                                                                                                                                               |
| <b>Action</b>                | <p>Use the following operational mode commands to verify that a three-color policer is working properly:</p> <ul style="list-style-type: none"><li>• <b>show class-of-service forwarding-table classifiers</b></li><li>• <b>show interfaces <i>interface-name</i> extensive</b></li><li>• <b>show interfaces queue <i>interface-name</i></b></li></ul> |
| <b>Related Documentation</b> | <ul style="list-style-type: none"><li>• <a href="#">Overview of Policers on page 51</a></li><li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 69</a></li></ul>                                                                                                                                         |

---

## Troubleshooting Policer Configuration

- [Incomplete Count of Packet Drops on page 72](#)
- [Counter Reset When Editing Filter on page 73](#)
- [Invalid Statistics for Policer on page 73](#)
- [Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured on page 73](#)
- [Filter-Specific Egress Policers on QFX3500 Devices Might Allow More Throughput Than Is Configured on page 74](#)
- [Policers Can Limit Egress Filters on page 75](#)

### Incomplete Count of Packet Drops

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Problem</b> | <p><b>Description:</b> Under certain circumstances, Junos OS might display a misleading number of packets dropped by an ingress policer.</p> <p>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</p> |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

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 25](#) 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:** On some switches, the number of egress policers that you configure can affect the total number of allowed egress firewall filters. (This issue does not affect QFX10000 switches.) On the affected switches, 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

# Configuring Port Security

- [Port Security on page 79](#)



## CHAPTER 3

# Port Security

- [Overview of Access Port Protection on page 79](#)
- [Understanding MAC Limiting and MAC Move Limiting for Port Security on page 81](#)
- [Verifying That MAC Limiting Is Working Correctly on page 83](#)
- [Verifying That MAC Move Limiting Is Working Correctly on page 86](#)
- [Verifying That the Port Error Disable Setting Is Working Correctly on page 86](#)
- [Configuring Persistent MAC Learning \(CLI Procedure\) on page 87](#)
- [Understanding Trusted and Untrusted Ports on page 89](#)
- [Understanding Trusted DHCP Servers for Port Security on page 89](#)
- [Verifying That a Trusted DHCP Server Is Working Correctly on page 89](#)
- [Understanding DHCP Option 82 for Port Security on page 91](#)
- [Understanding Static ARP Entries on page 93](#)

## Overview of Access Port Protection

---

Port security features on QFX10000 switches 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 79](#)
- [Mitigation of Rogue DHCP Server Attacks on page 80](#)
- [Protection Against DHCP Starvation Attacks on page 80](#)

## 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 DHCPOFFER 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 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 81](#)
  - [Configuring MAC Limiting](#)
  - [Verifying That MAC Limiting Is Working Correctly on page 83](#)

## 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 81](#)
- [MAC Move Limiting on page 82](#)
- [Actions for MAC Limiting on page 82](#)
- [MAC Addresses That Exceed the MAC Limit or MAC Move Limit on page 82](#)

### 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 83](#).

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 *mac-limit* for more information.

## 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 Features to Protect the Access Ports on Your Device Against the Loss of Information and Productivity*
- *Configuring MAC Limiting*
- *Configuring MAC Move Limiting (CLI Procedure)*

- [Verifying That MAC Limiting Is Working Correctly on page 83](#)
- [Verifying That MAC Move Limiting Is Working Correctly on page 86](#)
- *Example: Configuring Basic Port Security Features*
- [no-allowed-mac-log on page 190](#)

---

## 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 83](#)
2. [Verifying That Allowed MAC Addresses Are Working Correctly on page 84](#)
3. [Verifying That Interfaces Are Shut Down on page 84](#)
4. [Customizing the Ethernet Switching Table Display to View Information for a Specific Interface on page 85](#)

## 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 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 expires.

- Related Documentation**
- [Understanding MAC Limiting and MAC Move Limiting for Port Security on page 81](#)
  - [port-error-disable on page 192](#)

## Configuring Persistent MAC Learning (CLI Procedure)



**NOTE:** This topic uses Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Configuring Persistent MAC Learning (CLI Procedure)*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

Persistent MAC address learning is disabled by default. You can enable it to:

- Help prevent traffic losses for trusted workstations and servers because, if persistent MAC address learning is enabled on an interface, the interface does not have to relearn the addresses from ingress traffic after a restart.
- Protect the switch against security attacks—Use persistent MAC learning in combination with MAC limiting to protect against attacks while still obviating the need to statically configure MAC addresses. When the initial learning of MAC addresses up to the number specified by the MAC limit is done, new addresses are not allowed even after a restart.

The port is secured because after the limit has been reached, additional devices cannot connect to the interface.

To configure persistent MAC learning on an interface and limit the number of allowed MAC addresses:

1. Enable persistent MAC learning on an interface:

```
[edit switch-options]
user@switch# set interface interface-name persistent-learning
```

2. Configure the MAC limit on an interface, and specify the action that the switch takes after the specified limit is exceeded:

```
[edit switch-options]
user@switch# set interface interface-name interface-mac-limit limit packet-action action
```

After you set a new MAC limit for the interface, the system clears existing entries in the MAC address forwarding table associated with the interface.

Values for *action* are:

**drop**—Drop packets with new source MAC addresses, and do not learn the new source MAC addresses.

**drop-and-log**—(EX Series switches only) Drop packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.

**log**—(EX Series switches only) Hold packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.

**none**—(EX Series switches only) Forward packets with new source MAC addresses, and learn the new source MAC address.

**shutdown**—(EX Series switches only) Disable the specified interface, and generate an alarm, an SNMP trap, or a system log entry.



**TIP:** If you move a device within your network that has a persistent MAC address entry on the switch, use the `clear ethernet-switching table persistent-mac` command to clear the persistent MAC address entry from the interface. If you move the device and do not clear the persistent MAC address from the original port it was learned on, then the new port will not learn the MAC address of the device and the device will not be able to connect.

If the original port is down when you move the device, then the new port will learn the MAC address and the device can connect. However, if you do not clear the persistent MAC address on the original port, then when the port restarts, the system reinstalls the persistent MAC address in the forwarding table for that port. If this occurs, the persistent MAC address is removed from the new port and the device loses connectivity.

---

**Related Documentation**

- *Configuring Persistent MAC Learning (CLI Procedure)*

- *Configuring MAC Move Limiting (CLI Procedure)*
- *Understanding Persistent MAC Learning (Sticky MAC)*

## 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 Monitoring DHCP Messages Received from Untrusted Devices*
  - *Example: Configuring Basic Port Security Features*

## 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 91](#)
- [Suboption Components of Option 82 on page 92](#)
- [Configurations That Support Option 82 on page 92](#)

### 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 92](#) 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.

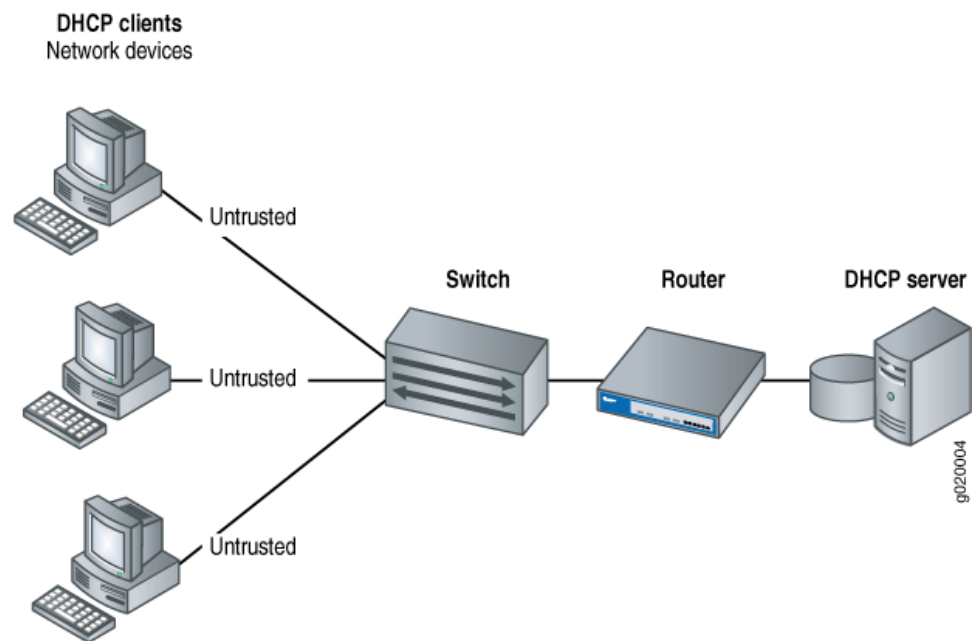
## Configurations That Support Option 82

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 4 on page 93](#) illustrates a scenario for the switch-as-relay-agent; in this instance, the switch relays requests through a router to the server.



Figure 4: Switch Relays DHCP Requests to Server



For the configuration shown in [Figure 4 on page 93](#), you set DHCP option 82 at the **[edit forwarding-options helpers bootp]** hierarchy level.

#### Related Documentation

- *Overview of Access Port Protection*
- *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 4

# Configuring Device Security

- [Device Security on page 97](#)



## CHAPTER 4

# Device Security

- [Understanding Storm Control on page 97](#)
- [Example: Configuring Storm Control to Prevent Network Outages on page 98](#)
- [Verifying That the Port Error Disable Setting Is Working Correctly on page 101](#)
- [Understanding Unicast RPF on page 102](#)
- [Configuring Unicast RPF \(CLI Procedure\) on page 106](#)
- [Disabling Unicast RPF \(CLI Procedure\) on page 107](#)
- [Verifying Unicast RPF Status on page 108](#)
- [Understanding Unknown Unicast Forwarding on page 111](#)
- [Configuring Unknown Unicast Forwarding \(CLI Procedure\) on page 111](#)

### 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**

- [action-shutdown on page 172](#)
- [port-error-disable on page 192](#)
- *storm-control*

---

## 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.

- [Requirements on page 99](#)
- [Overview and Topology on page 99](#)
- [Configuration on page 100](#)

## 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 97](#)
- [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 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 expires.

**Related Documentation**

- [Understanding MAC Limiting and MAC Move Limiting for Port Security on page 81](#)
- [port-error-disable on page 192](#)

## 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, by default 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. You can also enable loose mode, which means that the system checks to see if the packet has a source address with a corresponding prefix in the routing table but does not check whether the receiving interface is the best return path to the packet's unicast source address.



**NOTE:** On Juniper Networks EX3200, EX4200, and EX4300 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, and EX4300 Switches” on page 105.](#)

This topic covers:

- [Unicast RPF for Switches Overview on page 102](#)
- [Unicast RPF Implementation on page 103](#)
- [When to Enable Unicast RPF on page 103](#)
- [When Not to Enable Unicast RPF on page 104](#)
- [Limitations of the Unicast RPF Implementation on EX3200, EX4200, and EX4300 Switches on page 105](#)

### 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 103.](#))

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 103](#)
- [Bootstrap Protocol \(BOOTP\) and DHCP Requests on page 103](#)
- [Default Route Handling on page 103](#)

---

### 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.

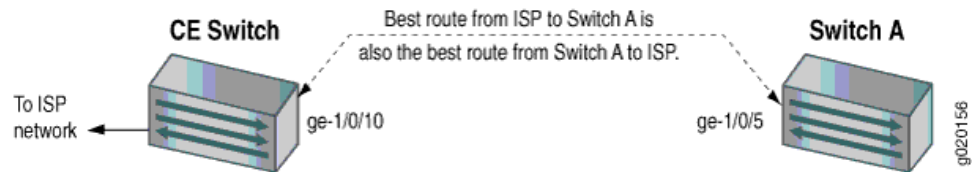
## When to Enable Unicast RPF

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 5 on page 104](#). 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 5: 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, and EX4300 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.

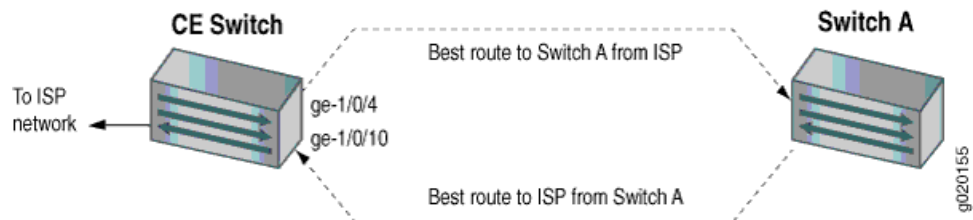
## When Not to Enable Unicast RPF

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 6 on page 105](#). 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 6: Asymmetrically Routed Interfaces**



**NOTE:** Do not enable unicast RPF on EX3200, EX4200, and EX4300 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, and EX4300 Switches

On EX3200, EX4200, and EX4300 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 106](#)
  - [Disabling Unicast RPF \(CLI Procedure\) on page 107](#)

---

## 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. When you enable unicast RPF, by default 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. You can also enable loose mode, which means that the system checks to see if the packet has a source address with a corresponding prefix in the routing table but does not check whether the receiving interface is the best return path to the packet's unicast source address.



**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 interface-name unit 0 family inet rpf-check
```

To enable unicast RPF loose mode, enter:

```
[edit interfaces]
user@switch# set interface-name unit 0 family inet rpf-check mode loose
```



**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 108](#)
- [Disabling Unicast RPF \(CLI Procedure\) on page 107](#)
- [Troubleshooting Unicast RPF](#)
- [Understanding Unicast RPF on page 102](#)

## 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 108](#)
- [Configuring Unicast RPF \(CLI Procedure\) on page 106](#)
- [Understanding Unicast RPF on page 102](#)

## Verifying Unicast RPF Status

- |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b> | Verify that unicast reverse-path forwarding (RPF) is enabled and is working on the interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Action</b>  | <p>Use one of the <b>show interfaces <i>interface-name</i></b> commands with either the <b>extensive</b> or <b>detail</b> options to verify that unicast RPF is enabled and working on the switch. The following example displays output from the <b>show interfaces ge- extensive</b> command.</p> <pre>user@switch&gt; 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</pre> |



```

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:
 Total octets Receive Transmit
 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
 Jabber frames 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 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
 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 106](#)

- [Disabling Unicast RPF \(CLI Procedure\) on page 107](#)
- *Troubleshooting Unicast RPF*

## 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 traverse a VLAN to all interfaces that are members of that 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 flooding of packets is known as a traffic storm.

To prevent a traffic storm, you can disable the flooding of unknown unicast packets to all VLAN interfaces by configuring specific VLANs or all VLANs to forward all unknown unicast traffic traversing them to a specific interface. You can configure multiple VLANs to forward unknown unicast packets to the same interface or configure different interfaces for different VLANs. This channels the unknown unicast traffic traversing VLANs to specific interfaces instead of flooding all interfaces.

### Related Documentation

- *Configuring Unknown Unicast Forwarding (CLI Procedure)*
- [Configuring Unknown Unicast Forwarding \(CLI Procedure\) on page 111](#)
- *Understanding Storm Control on EX Series Switches*
- *Understanding Storm Control for Managing Traffic Levels on Switching Devices*
- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*

## 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 that traverse a VLAN to all interfaces associated with that VLAN. This flooding of packets is known as a traffic storm and can negatively impact network performance.

To prevent flooding unknown unicast traffic across the switch, configure unknown unicast forwarding to direct all unknown unicast packets within a VLAN to a specific interface.

You can configure each VLAN to divert unknown unicast traffic to a different interface or use the same interface for multiple VLANs.

- [Configuring Unknown Unicast Forwarding on EX4300 Switches on page 112](#)
- [Configuring Unknown Unicast Forwarding on EX9200 Switches on page 112](#)

## Configuring Unknown Unicast Forwarding on EX4300 Switches

To configure unknown unicast forwarding options on EX4300 switches:

- Configure unknown unicast forwarding for a specific VLAN 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 interface-name
```

- Configure unknown unicast forwarding for all VLANs and specify the interface to which all unknown unicast traffic will be forwarded:

```
[edit switch-options]
user@switch# set unknown-unicast-forwarding vlan all interface interface-name
```

## Configuring Unknown Unicast Forwarding on EX9200 Switches

To configure unknown unicast forwarding on EX9200 switches, you must configure a flood filter and apply it to VLANs for which you want to configure unknown unicast forwarding. Flood filters are firewall filters that are applied only to broadcast, unknown unicast, and multicast (BUM) traffic. If a flood filter is configured, only traffic packets that are of the packet type **unknown-unicast** are forwarded to the interface on which unicast forwarding is configured. A next-hop group redirects the packets according to the action specified in the flood filter.

To configure the next-hop group that receives Layer 2 packets and then configure the interface to which these packets are forwarded:

1. Configure the **next-hop-group** action for the Layer 2 interface expected to receive unknown unicast packets:

```
[edit forwarding-options]
user@switch# set next-hop-group next-hop-group-name group-type layer-2
[edit forwarding-options]
user@switch# set next-hop-group next-hop-group-name interface interface-name
```

For example:

```
[edit forwarding-options]
user@switch# set next-hop-group uuf-nhg group-type layer-2
[edit forwarding-options]
user@switch# set next-hop-group uuf-nhg interface ge-3/1/7.0
```

2. Configure a firewall filter with family address type **ethernet-switching**:

```
[edit firewall]
user@switch# set family ethernet-switching filter filter-name
```

For example:

```
[edit firewall]
user@switch# set family ethernet-switching filter uuf_filter
```

3. Configure a term in the firewall filter for the interface that receives unknown unicast packets (the interface specified in Step 1) to discard unknown unicast packets:

```
[edit firewall family ethernet-switching filter filter-name]
user@switch# set term term-name from interface interface-name
user@switch# set term term-name from traffic-type unknown-unicast
user@switch# set term term-name then discard
```

For example:

```
[edit firewall family ethernet-switching filter uuf_filter]
user@switch# set term source-drop from interface ge-3/1/7.0
user@switch# set term source-drop from traffic-type unknown-unicast
user@switch# set term source-drop then discard
```

4. Configure a term in the firewall filter for unknown unicast packets to be flooded to the interface enabled for unknown unicast forwarding by using **next-hop-group** (in step 1):

```
[edit firewall family ethernet-switching filter filter-name]
user@switch# set term term-name from traffic-type unknown-unicast
user@switch# set term term-name then next-hop-group group-name
```

For example:

```
[edit firewall family ethernet-switching filter uuf_filter]
user@switch# set term uuf-flood from traffic-type unknown-unicast
user@switch# set term uuf-flood then next-hop-group uuf-nhg
```

5. Configure a default term for the firewall filter to forward packets other than unknown unicast packets:

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

For example:

```
[edit firewall family ethernet-switching filter uuf_filter]
user@switch# set term fwd-default then accept
```

6. Apply the filter as a flood filter on the VLAN that includes the interface which will receive unknown unicast packets:

```
[edit vlans vlan-name]
user@switch# set forwarding-options flood input filter-name
```

For example:

```
[edit vlans v1]
user@switch# set forwarding-options flood input uuf_filter
```

#### Related Documentation

- [Understanding Unknown Unicast Forwarding on page 111](#)
- [Verifying That Unknown Unicast Packets Are Forwarded to a Single Interface](#)



## PART 5

# DDoS Protection

- [Overview of DDoS Protection on page 117](#)
- [Configuring DDoS Protection on page 121](#)
- [Monitoring DDoS Protection on page 135](#)





## CHAPTER 5

# Overview of DDoS Protection

- [Understanding Distributed Denial-of-Service Protection on QFX Series Switches on page 117](#)

### 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 both QFX10000 switches and QFX5200 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 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 Types and Packet Priorities

DDoS protection includes two types of policers:

- An *aggregate policer* is applied to the complete set of packet types that belong to a protocol group. For example, you can configure an aggregate policer that applies to all RADIUS control packet types or to all DHCP control packet types. You can specify bandwidth and burst limits for aggregate policers. An aggregate policer is available for all protocol groups. Aggregate policers are supported by all protocol groups.
- An *individual policer*, also referred to as a *packet-type policer*, is allocated for a specific control packet type within a protocol group. For example, you can configure a policer for one or more types of RADIUS control packets. You can specify bandwidth and burst limits, prioritize one packet type over another, and enable a packet type to bypass the aggregate policer for the protocol group.

Individual policers are not available for all protocol groups. See [protocols](#) for a list of protocol groups that have individual policers.

A control packet is policed first by its individual policer (if supported) and then by its aggregate policer. A packet dropped by the individual policer never reaches the aggregate policer. A packet that passes the individual policer can subsequently be dropped by the aggregate policer.

Each packet type within a protocol group has a default, configurable priority: low, medium, or high. Each control packet competes with other packets for the bandwidth within the limit imposed by its aggregate policer based on the priority configured for each packet type in the protocol group.

The priority mechanism is absolute. High-priority traffic gets bandwidth in preference to medium-priority and low-priority traffic. Medium-priority traffic gets bandwidth in preference to low-priority traffic. Low-priority traffic can use only the bandwidth left by high-priority and medium-priority traffic. If higher-priority traffic takes all of the bandwidth, then all the lower-priority traffic is dropped.

## Example of Policer Priority Behavior

For example, consider how you might configure packet types within the RADIUS protocol group. Suppose you configure individual policers for accounting and authorization packets, as well as a RADIUS aggregate policer for all RADIUS control packets. You might want to prioritize the RADIUS authorization function over the RADIUS accounting function, and therefore you would assign a high priority to the authorization control packets and a low priority to accounting control packets.

The aggregate policer imposes a total bandwidth limit for the protocol group. Authorization packets passed by their individual policer have access to that bandwidth before accounting packets passed by their individual policer, because the authorization packets have a higher priority. If enough authorization packets are passed that they use all the available bandwidth, then all the accounting packets are dropped, because there is no bandwidth remaining at the aggregate policer.

## Policer Enforcement Points on QFX Series Switches

On both QFX1000 and QFX5200 switches, the DDoS policers operate at the line card level. Control traffic arriving from all ports of a line card 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 Protection Against DDoS Attacks on page 121](#)
  - [Verifying and Managing DDoS Protection on page 135](#)



## CHAPTER 6

# Configuring DDoS Protection

- [Configuring Protection Against DDoS Attacks on page 121](#)
- [Example: Configuring DDoS Protection on QFX Series Switches on page 122](#)
- [Disabling DDoS Protection Policers and Logging Globally on page 126](#)
- [Configuring DDoS Protection Policers on QFX Series Switches on page 126](#)
- [Tracing DDoS Protection Operations on page 130](#)

## Configuring Protection Against DDoS Attacks

---

DDoS protection is enabled by default for all supported protocol groups and packet types. Default values are present for bandwidth, bandwidth scale, burst, burst scale, priority, and recover time. You can change the DDoS configuration for individual packet types within a protocol group or for the aggregate policer for the protocol group. DDoS logging is enabled by default, but you can disable it globally for all DDoS events or for individual packet types within a protocol group. You can also fine-tune monitoring of DDoS events by configuring tracing operations.

You can disable DDoS protection at the Routing Engine and for all line cards either globally or for individual packet types within a protocol group.



**NOTE:** DDoS protection is supported only on MX Series routers that have only MPCs installed, T4000 routers that have only FPC5s installed, EX9200 switches, QFX5200 switches, and QFX10000 switches. If the router platforms have other line cards in addition to MPCs (MX Series) or FPC5s (T4000), the CLI accepts the configuration but the other line cards are not protected and so the router is not protected. Neither QFX10002 switches nor QFX5200 switches support policers at the Routing Engine.

---

To configure DDoS protection:

1. (Optional) Configure global DDoS settings.  
[See “Disabling DDoS Protection Policers and Logging Globally” on page 126.](#)
2. (Optional) Configure DDoS settings for individual packet types.

For MX Series routers, T4000 routers, or EX9200 switches, see *Configuring DDoS Protection Policers for Individual Packet Types*. For QFX10000 switches, see “[Configuring DDoS Protection Policers on QFX Series Switches](#)” on page 126.

3. (Optional) Configure tracing for DDoS operations.

See *Tracing DDoS Protection Operations*.

**Related Documentation**

- *Distributed Denial-of-Service (DDoS) Protection Overview*
- [Understanding Distributed Denial-of-Service Protection on QFX Series Switches on page 117](#)
- *Example: Configuring DDoS Protection*
- [Example: Configuring DDoS Protection on QFX Series Switches on page 122](#)

---

## 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 122](#)
- [Overview on page 122](#)
- [Configuration on page 123](#)
- [Verification on page 124](#)

### Requirements

DDoS protection requires the following hardware and software:

- QFX Series switch that supports DDoS protection
- Junos OS Release 15.1X53-D10 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, configuring policers for particular control packet types within 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 radius aggregate bandwidth 150
set ddos-protection protocols radius aggregate burst 2000
set ddos-protection protocols radius accounting bandwidth 100 burst 150
set ddos-protection protocols radius accounting priority low
set ddos-protection protocols radius server bypass-aggregate
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 radius
```
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 radius]
user@host# set aggregate bandwidth 150
```
3. Configure the maximum burst rate for the RADIUS aggregate policer.  

```
[edit system ddos-protection protocols radius]
user@host# set aggregate burst 2000
```
4. Configure a different maximum traffic rate and burst size for RADIUS accounting packets.  

```
[edit system ddos-protection protocols radius]
user@host# set accounting bandwidth 100 burst 1500
```
5. Decrease the priority for RADIUS accounting packets.  

```
[edit system ddos-protection protocols radius]
user@host# set accounting priority low
```
6. Prevent RADIUS server control packets from being included in the aggregate bandwidth; that is, server packets do not contribute toward the combined RADIUS traffic to determine whether the aggregate bandwidth is exceeded. However, the server packets are still included in traffic rate statistics.

```
[edit system ddos-protection protocol radius]
user@host# set server bypass-aggregate
```

7. 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 {

 radius {
 aggregate {
 bandwidth 150;
 burst 2000;
 }
 server {
 bypass-aggregate;
 }
 accounting {
 bandwidth 100;
 burst 1500;
 priority low;
 }
 }
}
```

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 124](#)

---

### Verifying the DDoS Protection Configuration

**Purpose** Verify that the RADIUS policer values have changed from the default.

**Action** From operational mode, enter the **show ddos-protection protocols radius parameters** command.

```
user@host> show ddos-protection protocols radius parameters
Packet types: 5, Modified: 3
* = User configured value
```



## Protocol Group: Radius

```

Packet type: aggregate (Aggregate for all Radius 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

Packet type: server (Radius server traffic)
Individual policer configuration:
 Bandwidth: 200 pps
 Burst: 2048 packets
 Priority: High
 Recover time: 300 seconds
 Enabled: Yes
 Bypass aggregate: Yes*
Routing Engine information:
 Bandwidth: 200 pps, Burst: 2048 packets, enabled
FPC slot 0 information:
 Bandwidth: 100% (200 pps), Burst: 100% (2048 packets), enabled

Packet type: accounting (Radius accounting traffic)
Individual policer configuration:
 Bandwidth: 100 pps*
 Burst: 1500 packets*
 Priority: Low*
 Recover time: 300 seconds
 Enabled: Yes
 Bypass aggregate: No
Routing Engine information:
 Bandwidth: 100 pps, Burst: 1500 packets, enabled
FPC slot 0 information:
 Bandwidth: 100% (100 pps), Burst: 100% (1500 packets), enabled

Packet type: authorization (Radius authorization traffic)
Individual policer configuration:
 Bandwidth: 200 pps
 Burst: 2048 packets
 Priority: High
 Recover time: 300 seconds
 Enabled: Yes
 Bypass aggregate: No
Routing Engine information:
 Bandwidth: 200 pps, Burst: 2048 packets, enabled
FPC slot 0 information:
 Bandwidth: 100% (200 pps), Burst: 100% (2048 packets), enabled

```

**Meaning** The command output shows the current configuration of the RADIUS aggregate policer and the RADIUS accounting, server, and authorization control packet policers. Policers 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.

- Related Documentation**
- [Understanding Distributed Denial-of-Service Protection on QFX Series Switches on page 117](#)
  - [Configuring Protection Against DDoS Attacks on page 121](#)

---

## Disabling DDoS Protection Policers and Logging Globally

---

DDoS policers are enabled by default for all supported protocol groups and packet types.

On MX Series routers, T4000 routers, and EX9200 switches, 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.

On both QFX10002 switches and QFX5200 switches, policers are established at the level of individual line cards only. If you disable line-card policers globally, DDoS protection is disabled on 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 or switch.



**NOTE:** The global configuration for disabling policers and logging overrides any local configuration for packet types.

To configure global DDoS settings:

1. (Optional) Disable line card policers.  

```
[edit system ddos-protection global]
user@host# set disable-fpc
```
2. (Optional) Disable Routing Engine policers (not supported on QFX10002 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 on page 121](#)

---

## 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.
- Modify the policer bandwidth and burst values for individual control packet types within a protocol group, for those groups that support policers for individual packet types. You can specify that packets of a certain type have a higher or lower priority than other types. You can also specify that a packet type bypass the aggregate policer for the protocol group. See [protocols](#) for the supported packet types and their default policer values.
- Scale the bandwidth and burst values for a policer on a line card so that the policer triggers at lower thresholds than the overall protocol thresholds.
- Disable logging for a specific policer.
- Disable a policer on all line cards or on an individual line card. On devices with a single line card, disabling policers on the line card 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 127](#)
- [Configuring Packet-Type Policers for a Protocol Group on page 128](#)
- [Configuring Policers on Individual Line Cards on page 129](#)
- [Disabling Policers and Policer Logging on page 129](#)

## 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 Packet-Type Policers for a Protocol Group

Some protocol groups allow you to configure a separate policer for each control packet type. Control traffic is subject first to the packet-type policer and then to the aggregate policer.

To configure a packet-type policer:

1. Specify the protocol group and packet type.

```
[edit system ddos-protection protocols]
user@host# edit protocol-group packet-type
```

For example, to specify the RADIUS protocol group and the authorization packet type:

```
[edit system ddos-protection protocols]
user@host# edit radius authorization
```

2. (Optional) Configure the maximum traffic rate the policer allows for the packet type.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set bandwidth packets-per-second
```

For example, to set a bandwidth of 150 packets per second for RADIUS authorization packets:

```
[edit system ddos-protection protocols radius authorization]
user@host# set bandwidth 150
```

3. (Optional) Configure the maximum number of packets of the packet type that the policer allows in a burst of traffic.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set burst size
```

For example, to set a maximum of 2000 RADIUS authorization packets:

```
[edit system ddos-protection protocols radius authorization]
```

```
user@host# set burst 2000
```

4. (Optional) Set the traffic priority—either high, medium, or low.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set priority level
```

For example, to specify a low priority for RADIUS accounting packets:

```
[edit system ddos-protection protocols radius accounting]
user@host# set priority low
```

5. (Optional) Allow packets of the specified type to bypass the aggregate policer.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set bypass-aggregate
```

For example, to bypass the aggregate policer for RADIUS server packets:

```
[edit system ddos-protection protocols radius server]
user@host# set bypass-aggregate
```

## Configuring Policers on Individual Line Cards

You can alter a policer behavior on a specific line card by scaling the policer's configured bandwidth and burst values. On switches with a single fixed line card, such as the QFX10002, scaling the policer values affects the entire switch.

- To scale the maximum bandwidth for a policer on a line card:

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type)]
user@host# set fpc slot-number bandwidth-scale percentage
```

For example, to scale the maximum bandwidth allowed by the DHCPv4v6 aggregate policer for the line card in slot 3 to 80 percent:

```
[edit system ddos-protection protocols dhcpv4v6 aggregate]
user@host# set fpc 3 bandwidth-scale 80
```

- To scale the maximum burst size for a policer on the line card:

```
[edit system ddos-protection protocols protocol-group (aggregate | packet-type)]
user@host# set fpc slot-number burst-scale percentage
```

For example, to scale the maximum burst size to 75 percent for the RADIUS server packets on the line card in slot 1:

```
[edit system ddos-protection protocols radius server]
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 a line card or line cards. Similarly, event logging by policers is enabled by default. You can selectively disable logging by a policer.

- To disable a policer on a specific line card:

```
[edit system ddos-protection protocols]
user@host# set protocol-group (aggregate | packet-type) fpc slot-number disable-fpc
```

For example, to disable the DDoS policers for the RADIUS authorization packet type on line card 3:

```
[edit system ddos-protection protocols]
user@host# set radius authorization fpc 3 disable-fpc
```

Because both QFX10002 and QFX5200 have a single line card, disabling a policer on that line card effectively disables it for the switch.

- To disable a policer on all line cards:

```
[edit system ddos-protection protocols]
user@host# set protocol-group (aggregate | packet-type) disable-fpc
```

For example, to disable the aggregate policer for the BFD protocol group on all line cards:

```
[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 | packet-type) 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

- [Configuring Protection Against DDoS Attacks on page 121](#)
- [Example: Configuring DDoS Protection on QFX Series Switches on page 122](#)

---

## 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 *Junos OS System Log Messages Reference*.)

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 131](#)
- [Configuring the Number and Size of DDoS Protection Log Files on page 131](#)
- [Configuring Access to the DDoS Protection Log File on page 132](#)
- [Configuring a Regular Expression for DDoS Protection Messages to Be Logged on page 132](#)
- [Configuring the DDoS Protection Tracing Flags on page 132](#)
- [Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged on page 133](#)

## Configuring the DDoS Protection Trace Log Filename

By default, the name of the file that records trace output for DDoS protection is **jddosd**. 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 on page 121](#)



# Monitoring DDoS Protection

- [Verifying and Managing DDoS Protection on page 135](#)

## 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 statistics packet-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 states packet-type**

**Related  
Documentation**

- *Verifying and Managing Flow Detection*

## PART 6

# Configuration Statements and Operational Commands

- [Configuration Statements \(Firewall Filters\) on page 139](#)
- [Configuration Statements \(Policers\) on page 151](#)
- [Configuration Statements \(Device Security\) on page 171](#)
- [Configuration Statements \(Port Security\) on page 183](#)
- [Configuration Statements \(DDoS Protection\) on page 197](#)
- [Operational Commands \(Firewall Filters\) on page 217](#)
- [Operational Commands \(Port Security\) on page 229](#)
- [Operational Commands \(DDoS Protection\) on page 231](#)



## CHAPTER 8

# Configuration Statements (Firewall Filters)

- [family on page 140](#)
- [filter on page 141](#)
- [filter \(Layer 2 and Layer 3 Interfaces\) on page 142](#)
- [filter \(VLANs\) on page 143](#)
- [firewall on page 144](#)
- [from on page 145](#)
- [input \(Forwarding Table\) on page 146](#)
- [interface-specific on page 146](#)
- [output \(Forwarding Table\) on page 147](#)
- [term on page 148](#)
- [then \(Filters\) on page 149](#)

## family

```
Syntax family family-name {
 filter filter-name {
 interface-specific;
 term term-name {
 from {
 match-conditions;
 }
 then {
 action;
 action-modifiers;
 }
 }
 }
 }
```

**Hierarchy Level** [edit [firewall](#)]

**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.  
**evpn** options introduced in Junos OS Release 15.1 for the MX Series.

**Description** Configure the fields a firewall filter can match on.

**Options** *family-name*—Type of addressing protocol:

- **ethernet-switching**—Filter Layer 2 Ethernet packets and Layer 3 (IP) packets (allows some Layer 3 filtering). Not supported on OCX Series switches.
- **evpn**—Filter Ethernet VPN (EVPN) packets.
- **inet**—Filter Layer 3 IPv4 packets (provides additional Layer 3 filter options).
- **inet6**—Filter Layer 3 IPv6 packets (provides additional Layer 3 filter options).
- **mpls**—Filter multiprotocol label switched packets. Not supported on OCX Series switches.

The remaining statements are explained separately.

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

**Related Documentation**

- *Firewall Filter Match Conditions and Actions*
- [Configuring Firewall Filters on page 30](#)
- [Overview of Firewall Filters on page 3](#)



## 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><i>Firewall Filter Match Conditions and Actions</i></li> <li><a href="#">Configuring Firewall Filters on page 30</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> | 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>• Configuring Gigabit Ethernet Interfaces (CLI Procedure)</li><li>• <a href="#">Configuring Firewall Filters on page 30</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.<br>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.                                                                                                                                                  |
| <b>Description</b>              | Apply a firewall filter to traffic entering or exiting 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 30</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</a></li> <li>• <a href="#">Configuring Firewall Filters on page 30</a></li> <li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 69</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</a></li> <li>• <a href="#">Configuring Firewall Filters on page 30</a></li> <li>• <a href="#">Understanding Firewall Filter Match Conditions on page 9</a></li> </ul>                                                      |

## input (Forwarding Table)

---

|                                 |                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>input <i>filter-name</i>;</code>                                                                                                                                                       |
| <b>Hierarchy Level</b>          | [edit forwarding-options family (inet   inet6   mpls   vpls) filter],<br>[edit routing-instances <i>routing-instance-name</i> forwarding-options family (inet   inet6   mpls   vpls) filter] |
| <b>Release Information</b>      | Statement introduced before Junos OS Release 7.4.<br>Statement introduced in Junos OS Release 15.1X53-D10 for QFX10000 switches..                                                            |
| <b>Description</b>              | Apply a forwarding table filter to ingress traffic of the forwarding table.                                                                                                                  |
| <b>Options</b>                  | <i>filter-name</i> —Name of the applied filter.                                                                                                                                              |
| <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="#">Applying Forwarding Table Filters</a></li></ul>                                                                                          |

## interface-specific

---

|                                 |                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>interface-specific;</code>                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit <a href="#">firewall family</a> <i>family-name</i> <a href="#">filter</a> <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</a></li><li>• <a href="#">Configuring Firewall Filters on page 30</a></li><li>• <a href="#">Overview of Firewall Filters on page 3</a></li></ul> |

## output (Forwarding Table)

---

|                                 |                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>output <i>filter-name</i>;</code>                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit forwarding-options family (inet   inet6   mpls) filter],<br>[edit routing-instances <i>routing-instance-name</i> forwarding-options family (inet   inet6   mpls) filter] |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 7.5.<br>Statement introduced in Junos OS Release 15.1X53-D10 for QFX10000 switches..                                                  |
| <b>Description</b>              | Configure filtering on the egress traffic of the forwarding table.                                                                                                             |
| <b>Options</b>                  | <i>filter-name</i> —Name of the applied filter.                                                                                                                                |
| <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>Applying Forwarding Table Filters</i></li> </ul>                                                                                   |

## term

---

|                                 |                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>term <i>term-name</i> {<br/>    from {<br/>        <i>match-conditions</i>;<br/>    }<br/>    then {<br/>        <i>action</i>;<br/>        <i>action-modifiers</i>;<br/>    }<br/>}</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> | 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>• <i>Firewall Filter Match Conditions and Actions</i></li><li>• <a href="#">Configuring Firewall Filters on page 30</a></li><li>• <a href="#">Overview of Firewall Filters on page 3</a></li></ul>                                           |



## then (Filters)

---

|                                 |                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> then {     action;     action-modifiers; } </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> | <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>• <i>Firewall Filter Match Conditions and Actions</i></li> <li>• <a href="#">Configuring Firewall Filters on page 30</a></li> <li>• <a href="#">Understanding Firewall Filter Match Conditions on page 9</a></li> </ul>                   |



## CHAPTER 9

# Configuration Statements (Policers)

- [action on page 152](#)
- [bandwidth-limit on page 152](#)
- [burst-size-limit on page 153](#)
- [color-aware on page 154](#)
- [color-blind on page 155](#)
- [committed-burst-size on page 156](#)
- [committed-information-rate on page 157](#)
- [excess-burst-size on page 158](#)
- [filter-specific on page 159](#)
- [firewall on page 160](#)
- [if-exceeding on page 161](#)
- [loss-priority high then discard \(Three-Color Policer\) on page 162](#)
- [peak-burst-size on page 163](#)
- [peak-information-rate on page 164](#)
- [policer on page 165](#)
- [single-rate on page 166](#)
- [then \(Policers\) on page 167](#)
- [three-color-policer on page 168](#)
- [two-rate on page 169](#)

## 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 69</a></li><li>• <a href="#">Overview of Policers on page 51</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 69</a></li><li>• <a href="#">Overview of Policers on page 51</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 51</a></li><li>• <a href="#">Understanding Color-Aware Mode for Single-Rate Tricolor Marking on page 58</a></li><li>• <a href="#">Understanding Color-Aware Mode for Two-Rate Tricolor Marking on page 60</a></li><li>• <a href="#">color-blind on page 155</a></li></ul>                                                                                                                                                                                                                                                                                                             |

## color-blind

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | color-blind;                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <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-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 51</a></li> <li>• <a href="#">Understanding Color-Blind Mode for Single-Rate Tricolor Marking on page 57</a></li> <li>• <a href="#">Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 60</a></li> <li>• <a href="#">Configuring Color-Blind Egress Policers for Medium-Low PLP on page 68</a></li> <li>• <a href="#">color-aware on page 154</a></li> </ul> |

## committed-burst-size

---

|                            |                                                                                                                                                                             |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>committed-burst-size bytes;</code>                                                                                                                                    |
| <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 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 69</a></li><li>• <a href="#">Overview of Policers on page 51</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 69</a></li> <li>• <a href="#">Overview of Policers on page 51</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 69</a></li><li>• <a href="#">Overview of Policers on page 51</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 69</a></li> <li>• <a href="#">Overview of Policers on page 51</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</a></li> <li>• <a href="#">Configuring Firewall Filters on page 30</a></li> <li>• <a href="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 69</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 <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>              | Configure policer rate limits.<br><br>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="#">Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 69</a></li> <li>• <a href="#">Overview of Policers on page 51</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 69</a></li><li>• <a href="#">Overview of Policers on page 51</a></li></ul>                                                                                                                                                                                                                                                                                                                                         |

## peak-burst-size

|                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                   | <code>peak-burst-size bytes;</code>                                                                                                                                                                                                                                                                      |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                          | [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 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 69</a></li> <li>• <a href="#">Overview of Policers on page 51</a></li> </ul>                                                                                        |

## peak-information-rate

---

|                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                                | <code>peak-information-rate <i>bits-per-second</i>;</code>                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>                                                                                                                                                                                                                                                                                                                       | [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 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>                                                                                                                                                                                                                                                                                                              | <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 69</a></li><li>• <a href="#">Overview of Policers on page 51</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 69</a></li> <li>• <a href="#">Configuring Firewall Filters on page 30</a></li> <li>• <a href="#">Overview of Policers on page 51</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 69</a></li><li>• <a href="#">Overview of Policers on page 51</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 69</a></li> <li>• <a href="#">Configuring Firewall Filters on page 30</a></li> <li>• <a href="#">Overview of Policers on page 51</a></li> </ul>                                              |

## three-color-policer

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>three-color-policer <i>policer-name</i> {<br/>    action {<br/>        loss-priority high then discard;<br/>    }<br/>    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/>    }<br/>    two-rate {<br/>        (color-aware   color-blind);<br/>        committed-information-rate <i>bps</i>;<br/>        committed-burst-size <i>bytes</i>;<br/>        peak-information-rate <i>bps</i>;<br/>        peak-burst-size <i>bytes</i>;<br/>    }<br/>}</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 69</a></li><li>• <a href="#">Overview of Policers on page 51</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 10

# Configuration Statements (Device Security)

- [action-shutdown on page 172](#)
- [bandwidth-level on page 173](#)
- [bandwidth-percentage on page 174](#)
- [interface \(Unknown Unicast Forwarding\) on page 175](#)
- [no-broadcast on page 176](#)
- [no-multicast on page 177](#)
- [no-unknown-unicast on page 178](#)
- [rpf-check on page 179](#)
- [storm-control on page 180](#)
- [storm-control-profiles on page 181](#)
- [unknown-unicast-forwarding on page 182](#)


## 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> |
| <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 97</a></li><li>• <i>Example: Configuring Storm Control to Prevent Network Outages</i></li><li>• <a href="#">port-error-disable on page 192</a></li><li>• <a href="#">clear ethernet-switching port-error on page 230</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>Range:</b> 100 through 100,000,000 on QFX10000 Series switches</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 174</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 173</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 <a href="#">unknown-unicast-forwarding</a> vlan <i>vlan-name</i>]</li> <li>For platforms without ELS:<br/>[edit ethernet-switching-options <a href="#">unknown-unicast-forwarding</a> 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 111</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 97</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 97</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 97</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 106</a></li> <li>• <a href="#">Disabling Unicast RPF (CLI Procedure) on page 107</a></li> <li>• <a href="#">Understanding Unicast RPF on page 102</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> <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.</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 for Managing Traffic Levels on Switching Devices</i></li></ul>                                                                                                         |



## storm-control-profiles

**Syntax** `storm-control-profiles profile-name {  
     action-shutdown;  
     all {  
         bandwidth-level;  
         bandwidth-percentage;  
         no-broadcast;  
         no-multicast;  
         no-registered-multicast;  
         no-unknown-unicast;  
         no-unregistered-multicast;  
     }  
 }`

**Hierarchy Level** [edit forwarding-options]

**Release Information** Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.  
 Statement introduced in Junos OS Release 13.2 for the QFX Series.  
 Statement introduced in Junos OS Release 14.1 for MX Series routers.

**Description** Configure a storm control profile on a switch or router. Storm control is used to prevent network outages that are caused by broadcast traffic storms. Storm control enables the switching device to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level—called the storm control level or storm control bandwidth—is exceeded, thus preventing packets from proliferating and degrading the LAN.



**NOTE:** The name of the storm control profile can contain no more than 127 characters.

The remaining statements are explained separately.

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

**Related Documentation**

- *Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches*
- *Understanding Storm Control for Managing Traffic Levels on Switching Devices*

## 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 111</a></li><li><a href="#">Understanding Unknown Unicast Forwarding on page 111</a></li></ul>                                                                                                                               |

## CHAPTER 11

# Configuration Statements (Port Security)

- [circuit-id on page 184](#)
- [fc-map on page 186](#)
- [fcoe-trusted on page 188](#)
- [mac-move-limit on page 189](#)
- [no-allowed-mac-log on page 190](#)
- [no-gratuitous-arp-request on page 191](#)
- [persistent-learning on page 191](#)
- [port-error-disable on page 192](#)
- [vendor-id on page 194](#)
- [write-interval on page 195](#)

## 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>                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                                 | <p> <b>NOTE:</b> When you configure <b>circuit-id</b>, <b>remote-id</b> is also enabled, even if you do not explicitly configure <b>remote-id</b> .</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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

- Related Documentation**
- *Configuring DHCP Option 82 to help Protect the Switching Devices Against Attacks (CLI Procedure)*
  - *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)*
  - *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>

## 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**
- *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 81](#)
  - *Configuring MAC Limiting*
  - *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>• <a href="#">Configuring Persistent MAC Learning (CLI Procedure) on page 87</a></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>              | <p>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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                                 | <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> | <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 MAC Limiting and MAC Move Limiting for Port Security on page 81</a></li> <li><a href="#">Understanding Storm Control on page 97</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 172](#)
- *disable-timeout*
- [clear ethernet-switching port-error on page 230](#)

## vendor-id

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                             | <code>vendor-id &lt;string&gt;;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>For Platforms with Enhanced Layer 2 Software (ELS)</b> | <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>For Platforms Without ELS</b>                          | <code>[edit ethernet-switching-options secure-access-port vlan (all   <i>vlan-name</i>) dhcp-option82],</code><br><code>[edit forwarding-options helpers bootp dhcp-option82],</code><br><code>[edit forwarding-options helpers bootp interface <i>interface-name</i> dhcp-option82]</code>                                                                                                                                                                                                                                                                                                                                     |
| <b>For MX Series Platforms</b>                            | <code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82]</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <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 <code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security]</code> 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 <code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security]</code> 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>                           | <b>system</b> —To view this statement in the configuration.<br><b>system-control</b> —To add this statement to the configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Related Documentation</b>                              | <ul style="list-style-type: none"> <li><i>Configuring DHCP Option 82 to help Protect the Switching Devices Against Attacks (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 dhcp-snooping-file]<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>• <i>Understanding DHCP Snooping for Monitoring DHCP Messages Received from Untrusted Devices</i></li></ul>                                                        |





## CHAPTER 12

# Configuration Statements (DDoS Protection)

- [bandwidth \(DDoS\) on page 198](#)
- [bandwidth-scale \(DDoS\) on page 199](#)
- [burst \(DDoS\) on page 200](#)
- [burst-scale \(DDoS\) on page 201](#)
- [bypass-aggregate \(DDoS\) on page 202](#)
- [ddos-protection \(DDoS\) on page 203](#)
- [disable-fpc \(DDoS\) on page 204](#)
- [disable-logging \(DDoS\) on page 205](#)
- [fpc \(DDoS\) on page 206](#)
- [global \(DDoS\) on page 207](#)
- [priority \(DDoS\) on page 208](#)
- [protocols \(DDoS\) on page 209](#)
- [traceoptions \(DDoS\) on page 214](#)

## bandwidth (DDoS)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>bandwidth <i>packets-per-second</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | <ul style="list-style-type: none"> <li>For MX Series routers, T4000 routers, and EX9200 switches:<br/>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i>)]</li> <li>For QFX10000 switches:<br/>[edit system ddos-protection <b>protocols</b> <i>protocol-group</i> (aggregate   <i>packet-type</i>)]</li> </ul>                                                                                                                                                                                                                                                                         |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>              | (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, or QFX10000 switches) Configure the DDoS bandwidth rate limit; that is, the maximum traffic rate (packets per second) allowed by the specified policer. When the value is exceeded, a violation is declared.                                                                                                                                                                                                                                                                                                                                   |
| <b>Options</b>                  | <p><b><i>packets-per-second</i></b>—Number of packets per second that are allowed by the aggregate or packet-type policer.</p> <p><b>Range:</b> 1 through 100,000 packets per second</p> <p><b>Default:</b> The default bandwidth value varies by packet type or protocol. You can view the default values for all packet types or protocols before you begin DDoS protection configuration by entering the <b>show ddos-protection protocols parameters brief</b> command from operational mode. For QFX10000 switches, the default bandwidth limits are also provided in the <b>protocols (DDoS)</b> statement description.</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 126</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                               |

## bandwidth-scale (DDoS)

|                                 |                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>bandwidth-scale <i>percentage</i>;</code>                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | <code>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i>) fpc <i>slot-number</i>]</code>                                                                                                                                                                                |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p> |
| <b>Description</b>              | (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, or QFX10000 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.                                               |
| <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 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>• <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 126</a></li> </ul>                                                                           |

## burst (DDoS)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>burst size;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | <ul style="list-style-type: none"> <li>For MX Series routers, T4000 routers, and EX9200 switches:<br/>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i>)]</li> <li>For QFX10000 switches:<br/>[edit system ddos-protection <a href="#">protocols</a> <i>protocol-group</i> (aggregate   <i>packet-type</i>)]</li> </ul>                                                                                                                                                                                                                          |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>                                                                                                                                                                                                                                                                           |
| <b>Description</b>              | (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, or QFX10000 switches) Configure the DDoS burst limit; that is, 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.                                                                                                                                                                                                                                                                                       |
| <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 or protocol. You can view the default values for all packet types or protocols on an unconfigured router or switch by entering the <b>show ddos-protection protocols parameters brief</b> command from operational mode. For QFX10000 switches, the default bandwidth limits are also provided in the <a href="#">protocols (DDoS)</a> statement description.</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 126</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                         |

## burst-scale (DDoS)

|                                 |                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>burst-scale <i>percentage</i>;</code>                                                                                                                                                                                                                                                                       |
| <b>Hierarchy Level</b>          | <code>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i>) fpc <i>slot-number</i>]</code>                                                                                                                                                                                |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p> |
| <b>Description</b>              | (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, or QFX10000 switches) Configure the percentage by which the DDoS burst limit is scaled down for the aggregate or packet-type policer on the card in the specified slot.                                                        |
| <b>Options</b>                  | <p><b><i>percentage</i></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>• <i>Configuring DDoS Protection Policers for Individual Packet Types</i></li> <li>• <a href="#">Configuring DDoS Protection Policers on QFX Series Switches on page 126</a></li> </ul>                                                                                    |

## bypass-aggregate (DDoS)

---

|                                 |                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | bypass-aggregate;                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | <ul style="list-style-type: none"><li>For MX Series routers, T4000 routers, and EX9200 switches:<br/>[edit system ddos-protection protocols <i>protocol-group packet-type</i>]</li><li>For QFX10000 and QFX5200 switches:<br/>[edit system ddos-protection <a href="#">protocols</a> <i>protocol-group packet-type</i>]</li></ul> |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>                 |
| <b>Description</b>              | (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, or QFX10000 switches) Prevent this packet type from being considered by the DDoS aggregate policer. Traffic for the packet type is still included in traffic statistics.                                                                       |
| <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 126</a></li></ul>                                                                                                  |

## ddos-protection (DDoS)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre> ddos-protection   global {     disable-fpc;     disable-logging;   }   protocols protocol-group (aggregate   packet-type) {     bandwidth packets-per-second;     burst size;     bypass-aggregate;     disable-fpc;     disable-logging;     fpc slot-number {       bandwidth-scale percentage;       burst-scale percentage;       disable-fpc;     }     priority level;   }   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>      | <p>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>              | <p>(QFX10000 and QFX5200 switches) 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 Protection Against DDoS Attacks on page 121</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 12.3R2 on EX9200 switches and T4000 routers.<br>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.<br>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.           |
| <b>Description</b>              | (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, QFX5200 switches, or QFX10000 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. |
| <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 126</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 126</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 12.3R2 on EX9200 switches and T4000 routers.<br>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.<br>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches. |
| <b>Description</b>              | (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, QFX5200 switches, or QFX10000 switches) Disable device-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 or for a protocol group. Typically used for debugging purposes.                                                                            |
| <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 126</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 126</a></li> <li>• <a href="#">Disabling Automatic Logging of Culprit Flow Events for a Packet Type</a></li> </ul>                                |

## fpc (DDoS)

|                                 |                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>fpc slot-number;   bandwidth-scale percentage;   burst-scale percentage;   disable-fpc; }</pre>                                                                                                                                                                                                                                                           |
| <b>Hierarchy Level</b>          | <ul style="list-style-type: none"> <li>For MX Series routers, T4000 routers, and EX9200 switches:<br/>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i>)]</li> <li>For QFX10000 and QFX5200 switches:<br/>[edit system ddos-protection <i>protocols protocol-group</i> (aggregate   <i>packet-type</i>)]</li> </ul> |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>                                              |
| <b>Description</b>              | (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, or QFX10000 switches) Modify the aggregate or packet-type policer on the specified line card.                                                                                                                                                                               |
| <b>Options</b>                  | <p><b>slot-number</b>—Slot number of the card.</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> | <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><i>Configuring DDoS Protection Policers for Individual Packet Types</i></li> <li><a href="#">Configuring DDoS Protection Policers on QFX Series Switches on page 126</a></li> </ul>                                                                                                                                     |

## global (DDoS)

|                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                                                                                                                                                              | <pre>global {   disable-fpc;   disable-logging;   disable-routing-engine;   flow-detection;   flow-report-rate;   violation-report-rate; }</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 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p> |
| <b>Description</b>                                                                                                                                                                                                                                                                                                                         | (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, QFX5200 switches, or QFX10000 switches) Modify DDoS policers, event logging, and flow detection globally for all protocols.                                                                                                    |
| <div>  <p><b>NOTE:</b> The following statements are not supported on QFX5200 and QFX10000 switches: <code>disable-routing-engine</code>, <code>flow-detection</code>, <code>flow-report-rate</code>, and <code>violation-report-rate</code>.</p> </div> |                                                                                                                                                                                                                                                                                                                   |
| The remaining statements are explained separately.                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                   |
| <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="#">Disabling DDoS Protection Policers and Logging Globally on page 126</a></li> </ul>                                                                                                                                                                           |

## priority (DDoS)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>priority level;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | <ul style="list-style-type: none"><li>For MX Series routers, T4000 routers, and EX9200 switches:<br/>[edit system ddos-protection protocols <i>protocol-group packet-type</i>]</li><li>For QFX10000 and QFX5200 switches:<br/>[edit system ddos-protection <a href="#">protocols</a> <i>protocol-group packet-type</i>]</li></ul>                                                                                                                                                            |
| <b>Release Information</b>      | <p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>                                                                                                                                                                            |
| <b>Description</b>              | (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, QFX5200 switches, or QFX10000 switches) Configure the priority for the packet type within the parent protocol group. In the event of downstream traffic congestion, high priority packets are provided bandwidth before medium priority packets. In turn, medium priority packets are provided bandwidth before low priority packets. Packets are dropped when there is insufficient available bandwidth. |
| <b>Options</b>                  | <i>level</i> —Priority of the packet type, low, medium, or high.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <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><i>Configuring DDoS Protection Policers for Individual Packet Types</i></li><li><a href="#">Configuring DDoS Protection Policers on QFX Series Switches on page 126</a></li></ul>                                                                                                                                                                                                                                                                      |

## protocols (DDoS)

```
Syntax protocols protocol-group (aggregate | packet-type) {
 bandwidth packets-per-second;
 burst size;
 bypass-aggregate;
 disable-fpc;
 disable-logging;
 fpc slot-number {
 bandwidth-scale percentage;
 burst-scale percentage;
 disable-fpc;
 }
 priority level;
}
```

**Hierarchy Level** [edit system [ddos-protection](#)]

**Release Information** Statement introduced in Junos OS Release 11.2.  
Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.  
Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

**Description** Configure DDoS policers for all packet types within a protocol group or for a particular packet type 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.

**packet-type**—Name of the control packet type to be policed. You can configure a packet-type policer only for the protocol groups listed in [Table 16 on page 209](#). For all other protocol groups, only aggregate policers are supported. [Table 16 on page 209](#) lists the packet-type policers and their default configuration.

**Table 16: Packet Types Supported by DDoS Protection on QFX Switches**

| Protocol Group | Packet Type   | Description                        | Default Bandwidth | Default Burst | Default Priority |
|----------------|---------------|------------------------------------|-------------------|---------------|------------------|
| mcast-snoop    | igmp          | Control packets for IGMP snooping  | 500               | 2048          | High             |
|                | mld           | Control packets for MLD snooping   | 500               | 2048          | High             |
|                | pim           | Control packets for PIM snooping   | 500               | 2048          | High             |
|                | unclassified  | Not supported on QFX10000 switches | —                 | —             | —                |
| radius         | accounting    | RADIUS accounting packets          | 200               | 2048          | High             |
|                | authorization | RADIUS authorization packets       | 200               | 2048          | High             |
|                | server        | RADIUS server traffic              | 200               | 2048          | High             |

***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 17 on page 211](#). The table shows the default configuration for the policers.

Table 17: Protocol Groups Supported by DDoS Protection on QFX Switches

| Protocol Group                 | Description                                                  | Default Bandwidth | Default Burst |
|--------------------------------|--------------------------------------------------------------|-------------------|---------------|
| <b>all-fiber-channel-enode</b> | Fiber channel ENode traffic                                  | 10                | 2048          |
| <b>arp</b>                     | ARP traffic                                                  | 500               | 1024          |
| <b>arp-snoop</b>               | ARP snooping traffic                                         | 500               | 2048          |
| <b>bfd</b>                     | Single-hop BFD traffic                                       | 1000              | 2048          |
| <b>bfdv6</b>                   | BFDv6 traffic                                                | 3000              | 10000         |
| <b>bgp</b>                     | BGP traffic                                                  | 1500              | 2048          |
| <b>bridge-control</b>          | Bridge Control traffic                                       | 10                | 2048          |
| <b>dhcpv4v6</b>                | DHCPv4 and DHCPv6 traffic (limits apply to combined traffic) | 500               | 2048          |
| <b>diameter</b>                | Diameter and Gx-Plus traffic                                 | 200               | 2048          |
| <b>dns</b>                     | DNS traffic                                                  | 200               | 2048          |
| <b>dtcp</b>                    | DTCP traffic                                                 | 200               | 2048          |
| <b>egpv6</b>                   | EGPv6 traffic                                                | 10                | 2048          |
| <b>ethernet-tcc</b>            | TCC-encapsulated Ethernet traffic                            | 100               | 2048          |
| <b>ftp</b>                     | FTP traffic                                                  | 500               | 2048          |
| <b>garp-reply</b>              | Gratuitous ARP reply traffic                                 | 100               | 2048          |
| <b>gre</b>                     | GRE traffic                                                  | 500               | 2048          |
| <b>icmp</b>                    | ICMP traffic                                                 | 500               | 2048          |
| <b>igmp</b>                    | IGMPv4 and IGMPv6 traffic                                    | 1000              | 2048          |
| <b>ip-options</b>              | IP traffic with IP packet header options                     | 100               | 2048          |
| <b>isis</b>                    | IS-IS traffic                                                | 1000              | 2048          |
| <b>iso-tcc</b>                 | TCC-encapsulated ISO traffic                                 | 100               | 2048          |
| <b>l2tp</b>                    | Layer 2 protocol tunneling traffic                           | 500               | 2048          |
| <b>lACP</b>                    | LACP traffic                                                 | 300               | 2048          |

Table 17: Protocol Groups Supported by DDoS Protection on QFX Switches (*continued*)

| Protocol Group         | Description                                        | Default Bandwidth | Default Burst |
|------------------------|----------------------------------------------------|-------------------|---------------|
| <b>ldp</b>             | LDP traffic                                        | 1000              | 200           |
| <b>ldp-hello</b>       | LDP hello packets                                  | 1000              | 2048          |
| <b>lldp</b>            | LLDP traffic                                       | 60                | 2048          |
| <b>lmp</b>             | LMP traffic                                        | 100               | 2048          |
| <b>martian-address</b> | Martian address                                    | 200               | 20            |
| <b>mcast-snoop</b>     | Control traffic for multicast snooping             | 500               | 2048          |
| <b>mld</b>             | MLD traffic                                        | 1000              | 2048          |
| <b>msdp</b>            | MSDP traffic                                       | 300               | 2048          |
| <b>multihop-bfd</b>    | Multihop BFD traffic                               | 1500              | 2048          |
| <b>ndpv6</b>           | NDPv6 traffic                                      | 500               | 1024          |
| <b>ntp</b>             | NTP traffic                                        | 200               | 2048          |
| <b>oam-cfm</b>         | OAM CFM traffic                                    | 200               | 2048          |
| <b>oam-lfm</b>         | OAM LFM traffic                                    | 200               | 2048          |
| <b>ospf</b>            | OSPF traffic                                       | 1000              | 200           |
| <b>ospf-hello</b>      | OSPF hello packets                                 | 1500              | 2048          |
| <b>pim-ctrl</b>        | PIM control packets                                | 1000              | 2048          |
| <b>pim-data</b>        | PIM data                                           | 2000              | 2048          |
| <b>proto-802-lx</b>    | 802.1X traffic                                     | 200               | 2048          |
| <b>ptp</b>             | PTP traffic                                        | 100               | 2048          |
| <b>pvstp</b>           | PVSTP traffic                                      | 2000              | 2048          |
| <b>radius</b>          | RADIUS traffic                                     | 200               | 2048          |
| <b>reject</b>          | Packets rejected by a next-hop forwarding decision | 100               | 2048          |
| <b>resolve</b>         |                                                    | 500               | 2048          |



Table 17: Protocol Groups Supported by DDoS Protection on QFX Switches (*continued*)

| Protocol Group | Description                                                                                             | Default Bandwidth | Default Burst |
|----------------|---------------------------------------------------------------------------------------------------------|-------------------|---------------|
|                | Unclassified IPv4 and IPv6 resolve packets sent to the host because of a traffic request resolve action |                   |               |
| <b>rip</b>     | RIP traffic                                                                                             | 100               | 2048          |
| <b>rsvp</b>    | RSVP traffic                                                                                            | 1000              | 2048          |
| <b>snmp</b>    | SNMP traffic                                                                                            | 500               | 2048          |
| <b>ssh</b>     | SSH traffic                                                                                             | 500               | 2048          |
| <b>stp</b>     | STP traffic                                                                                             | 2000              | 2048          |
| <b>tacacs</b>  | TACACS+ traffic                                                                                         | 200               | 2048          |
| <b>telnet</b>  | Telnet traffic                                                                                          | 500               | 2048          |
| <b>tll</b>     | Time to Live packets                                                                                    | 100               | 2048          |
| <b>vrrp</b>    | VRRP traffic                                                                                            | 1000              | 2048          |

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 126](#)

## 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 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Description</b>         | (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, QFX5200 switches, or QFX10000 switches) 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 <i>/var/log</i>.</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 graceful Routing Engine switchover (GRES).</li> <li>• <b>init</b>—Trace jddosd initialization.</li> <li>• <b>ipc</b>—Trace interface interprocess communication (IPC) messages.</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> </ul> |

- **signal**—Trace system signals that are passed to jddosd, such as SIGTERM.
- **socket**—Trace socket messages that are passed to jddosd from the Packet Forwarding Engine.
- **state**—Trace state machine events. This flag is not currently supported.
- **timer**—Trace jddosd timer events.
- **ui**—Trace user interface processing. This flag is not currently supported.

**level**—Level of tracing to perform. You can specify any of the following levels:

- **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> | trace—To view this statement in the configuration.                                            |
|                                 | trace-control—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 13

# Operational Commands (Firewall Filters)

- `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 39</a></li><li>• <a href="#">Verifying That Two-Color Policers Are Operational on page 71</a></li><li>• <a href="#">Overview of Firewall Filters on page 3</a></li><li>• <a href="#">Overview of Policers on page 51</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 39</a></li> <li>• <a href="#">Verifying That Two-Color Policers Are Operational on page 71</a></li> <li>• <a href="#">Overview of Firewall Filters on page 3</a></li> <li>• <a href="#">Overview of Policers on page 51</a></li> </ul>                                 |
| <b>List of Sample Output</b>    | <a href="#">show firewall on page 220</a><br><a href="#">show firewall filter <i>filter-name</i> on page 221</a><br><a href="#">show firewall counter <i>counter-name</i> on page 221</a><br><a href="#">show firewall log on page 221</a><br><a href="#">show firewall log detail on page 221</a>                                                                                  |
| <b>Output Fields</b>            | <a href="#">Table 18 on page 219</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 18: 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 18: 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><b>A</b>—Accept</li> <li><b>D</b>—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 39</a></li> <li>• <a href="#">Verifying That Two-Color Policers Are Operational on page 71</a></li> <li>• <a href="#">Overview of Firewall Filters on page 3</a></li> <li>• <a href="#">Overview of Policers on page 51</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show firewall policer on page 223</a><br><a href="#">show firewall policer policer-name on page 224</a>                                                                                                                                                                                                                                 |
| <b>Output Fields</b>            | <a href="#">Table 19 on page 223</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 19: 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 219</a></li> </ul>                                                                                        |
| <b>List of Sample Output</b>    | <a href="#">show interfaces filters on page 225</a><br><a href="#">show interfaces filters interface-name on page 226</a>                                                            |
| <b>Output Fields</b>            | <a href="#">Table 20 on page 225</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 20: 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
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 25</a></li> </ul>                                                                                                                                                                                                                                                                                            |
| <b>List of Sample Output</b>    | <a href="#">show pfe filter hw summary on page 228</a>                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Output Fields</b>            | <p><a href="#">Table 21 on page 227</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 21: 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 14

# Operational Commands (Port Security)

- `clear ethernet-switching port-error`

## 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 192</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.                                                                                                                                                                                                                                                                                                                                                           |

## CHAPTER 15

# Operational Commands (DDos Protection)

- `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`
- `show ddos-protection protocols violations`

## clear ddos-protection protocols

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>clear ddos-protection protocols</code><br><code>&lt;protocol-group &lt;packet-type&gt;&gt; (culprit-flows   states   statistics)</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | <p>Command introduced in Junos OS Release 11.2.</p> <p>Option <b>culprit-flows</b> introduced in Junos OS Release 12.3.</p> <p>Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <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.</p> <p><b>packet-type</b>—(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. This option is not supported on QFX Series switches.</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 234</a></li> <li>• <a href="#">show ddos-protection statistics on page 270</a></li> <li>• <a href="#">show ddos-protection version on page 272</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>List of Sample Output</b>    | <a href="#">clear ddos-protection protocols (Clear Statistics for All Protocols) on page 232</a><br><a href="#">clear ddos-protection protocols (Clear Violation States for Packet Type) on page 233</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 (Clear Statistics for All Protocols)

```
user@host> clear ddos-protection protocols statistics
```

**clear ddos-protection protocols (Clear Violation States for Packet Type)**

```
user@host> clear ddos-protection protocols radius server 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 12.3R2 on EX9200 switches and T4000 routers.  
Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.  
Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

**Description** Display DDoS protection configuration and statistics for protocol groups or individual packet types.

**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**—(Optional) Display DDoS protection information for the specified packet type in the protocol group. The available packet types vary by protocol group.  
On QFX10000 switches, only aggregate policers are available for protocol groups that are not in the following list:

- **mcast-snoop**—The following packet types are available for the **mcast-snoop** protocol group:
  - **igmp**—Control packets for IGMP snooping.
  - **mld**—Control packets for MLD snooping.
  - **pim**—Control packets for PIM snooping.
- **radius**—The following packet types are available for the **radius** protocol group:
  - **accounting**—RADIUS accounting packets.
  - **authorization**—RADIUS authorization packets.
  - **server**—RADIUS server traffic.

On MX Series routers, T4000 routers, and EX9200 switches, only aggregate policers are 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.
- **l2tp**—The following packet types are available for L2TP traffic:
  - **cdn**—Call-Disconnect-Notify message packets.
  - **hello**—Hello message packets.
  - **iccn**—Incoming-Call-Connected message packets.
  - **icrq**—Incoming-Call-Request message packets.
  - **scccn**—Start-Control-Connection-Connected message packets.
  - **sccrq**—Start-Control-Connection-Request message packets.
  - **stopccn**—Stop-Control-Connection-Notification message 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.
- **re-services**—The following packet type is available for Routing Engine-based HTTP redirect:
  - **captive-portal**—Routing Engine-based captive portal content delivery packets.
- **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 a protocol group.

[Table 22 on page 238](#) lists the protocol groups and the platforms they are supported on.

**Table 22: Supported Protocol Groups**

| Protocol Group                 | Description                 | MX Series Routers, T4000 Routers, EX9200 Switches | QFX10000 Switches |
|--------------------------------|-----------------------------|---------------------------------------------------|-------------------|
| <b>all-fiber-channel-enode</b> | Fiber channel ENode traffic | —                                                 | X                 |
| <b>amtv4</b>                   | IPv4 AMT traffic            | X                                                 | —                 |
| <b>amtv6</b>                   | IPv6 AMT traffic            | X                                                 | —                 |

Table 22: Supported Protocol Groups *(continued)*

| Protocol Group         | Description                    | MX Series Routers, T4000 Routers, EX9200 Switches | QFX10000 Switches |
|------------------------|--------------------------------|---------------------------------------------------|-------------------|
| <b>ancp</b>            | ANCP traffic                   | X                                                 | —                 |
| <b>ancpv6</b>          | ANCPv6 traffic                 | X                                                 | —                 |
| <b>arp</b>             | ARP traffic                    | X                                                 | X                 |
| <b>arp-snoop</b>       | ARP snooping traffic           | —                                                 | X                 |
| <b>atm</b>             | ATM traffic                    | X                                                 | —                 |
| <b>bfd</b>             | Single-hop BFD traffic         | X                                                 | X                 |
| <b>bfdv6</b>           | BFDv6 traffic                  | X                                                 | X                 |
| <b>bgp</b>             | BGP traffic                    | X                                                 | X                 |
| <b>bgpv6</b>           | BGPv6 traffic                  | X                                                 | —                 |
| <b>bridge-control</b>  | Bridge Control traffic         | —                                                 | X                 |
| <b>control</b>         | Control traffic                | X                                                 | —                 |
| <b>demux-autosense</b> | Demux autosensing traffic      | X                                                 | —                 |
| <b>dhcpv4</b>          | DHCPv4 traffic                 | X                                                 | —                 |
| <b>dhcpv6</b>          | DHCPv6 traffic                 | X                                                 | —                 |
| <b>dhcpv4v6</b>        | DHCPv4 and DHCPv6 traffic      | —                                                 | X                 |
| <b>diameter</b>        | Diameter and Gx-Plus traffic   | X                                                 | X                 |
| <b>dns</b>             | DNS traffic                    | X                                                 | X                 |
| <b>dtcp</b>            | DTCP traffic                   | X                                                 | X                 |
| <b>dynamic-vlan</b>    | Dynamic VLAN exception traffic | X                                                 | —                 |
| <b>egpv6</b>           | EGPv6 traffic                  | X                                                 | X                 |
| <b>eoam</b>            | EOAM traffic                   | X                                                 | —                 |
| <b>esmc</b>            | ESMC traffic                   | X                                                 | —                 |

Table 22: Supported Protocol Groups *(continued)*

| Protocol Group       | Description                                                                                               | MX Series Routers, T4000 Routers, EX9200 Switches | QFX10000 Switches |
|----------------------|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------|-------------------|
| <b>ethernet-tcc</b>  | TCC-encapsulated Ethernet traffic                                                                         | –                                                 | X                 |
| <b>fab-probe</b>     | Fab out probe packets                                                                                     | X                                                 | –                 |
| <b>filter-action</b> | IPv4 and IPv6 firewall filter action packets sent to the host because of reject terms in firewall filters | X                                                 | –                 |
| <b>firewall-host</b> | Firewall send-to-host traffic                                                                             | X                                                 | –                 |
| <b>frame-relay</b>   | Frame relay traffic                                                                                       | X                                                 | –                 |
| <b>ftp</b>           | FTP traffic                                                                                               | X                                                 | X                 |
| <b>ftpv6</b>         | FTPV6 traffic                                                                                             | X                                                 | –                 |
| <b>garp-reply</b>    | Gratuitous ARP reply traffic                                                                              | –                                                 | X                 |
| <b>gre</b>           | GRE traffic                                                                                               | X                                                 | X                 |
| <b>icmp</b>          | ICMP traffic                                                                                              | X                                                 | X                 |
| <b>igmp</b>          | IGMP traffic                                                                                              | X                                                 | X                 |
| <b>igmpv4v6</b>      | IGMP and MLD traffic                                                                                      | X                                                 | –                 |
| <b>igmpv6</b>        | MLD traffic                                                                                               | X                                                 | –                 |
| <b>inline-ka</b>     | Inline service interfaces keepalive traffic                                                               | X                                                 | –                 |
| <b>inline-svcs</b>   | Inline services traffic                                                                                   | X                                                 | –                 |
| <b>ip-fragments</b>  | IP fragments traffic                                                                                      | X                                                 | –                 |
| <b>ip-options</b>    | IP traffic with IP packet header options                                                                  | X                                                 | X                 |
| <b>isis</b>          | IS-IS traffic                                                                                             | X                                                 | X                 |
| <b>iso-tcc</b>       | TCC-encapsulated ISO traffic                                                                              | –                                                 | X                 |
| <b>jfm</b>           | JFM traffic                                                                                               | X                                                 | –                 |
| <b>keepalive</b>     | Keepalive traffic                                                                                         | X                                                 | –                 |

Table 22: Supported Protocol Groups (*continued*)

| Protocol Group         | Description                                | MX Series Routers, T4000 Routers, EX9200 Switches | QFX10000 Switches |
|------------------------|--------------------------------------------|---------------------------------------------------|-------------------|
| <b>l2tp</b>            | Layer 2 protocol tunneling traffic         | X                                                 | X                 |
| <b>lACP</b>            | LACP traffic                               | X                                                 | X                 |
| <b>ldp</b>             | LDP traffic                                | X                                                 | X                 |
| <b>ldp-hello</b>       | LDP hello packets                          | —                                                 | X                 |
| <b>ldpv6</b>           | LDPv6 traffic                              | X                                                 | —                 |
| <b>lldp</b>            | LLDP traffic                               | X                                                 | X                 |
| <b>lmp</b>             | LMP traffic                                | X                                                 | X                 |
| <b>lmpv6</b>           | LMPv6 traffic                              | X                                                 | —                 |
| <b>mac-host</b>        | Layer 2 MAC send-to-host traffic           | X                                                 | —                 |
| <b>martian-address</b> | Martian address                            | —                                                 | —                 |
| <b>mcast-snoop</b>     | Control traffic for multicast snooping     | X                                                 | X                 |
| <b>mld</b>             | MLD traffic                                | —                                                 | X                 |
| <b>mlp</b>             | MLP traffic                                | X                                                 | —                 |
| <b>msdp</b>            | MSDP traffic                               | X                                                 | X                 |
| <b>multihop-bfd</b>    | Multihop BFD traffic                       | —                                                 | X                 |
| <b>mld</b>             | MLD traffic                                | —                                                 | X                 |
| <b>msdpv6</b>          | MSDPv6 traffic                             | X                                                 | —                 |
| <b>multicast-copy</b>  | Host copy traffic due to multicast routing | X                                                 | —                 |
| <b>mvrp</b>            | MVRP traffic                               | X                                                 | —                 |
| <b>ndpv6</b>           | NDPv6 traffic                              | X                                                 | X                 |
| <b>ntp</b>             | NTP traffic                                | X                                                 | X                 |
| <b>oam-cfm</b>         | OAM CFM traffic                            | —                                                 | X                 |

Table 22: Supported Protocol Groups (*continued*)

| Protocol Group      | Description                                                              | MX Series Routers, T4000 Routers, EX9200 Switches | QFX10000 Switches |
|---------------------|--------------------------------------------------------------------------|---------------------------------------------------|-------------------|
| <b>oam-lfm</b>      | OAM LFM traffic                                                          | X                                                 | X                 |
| <b>ospf</b>         | OSPF traffic                                                             | X                                                 | X                 |
| <b>ospf-hello</b>   | OSPF hello packets                                                       | —                                                 | X                 |
| <b>ospfv3v6</b>     | OSPFv3/IPv6 traffic                                                      | X                                                 | —                 |
| <b>pfe-alive</b>    | Packet Forwarding Engine keepalive traffic                               | X                                                 | —                 |
| <b>pim</b>          | PIM traffic                                                              | X                                                 | —                 |
| <b>pim-ctrl</b>     | PIM control packets                                                      | —                                                 | X                 |
| <b>pim-data</b>     | PIM data                                                                 | —                                                 | X                 |
| <b>pimv6</b>        | PIMv6 traffic                                                            | X                                                 | —                 |
| <b>pmvrp</b>        | PMVRP traffic                                                            | X                                                 | —                 |
| <b>pos</b>          | POS traffic                                                              | X                                                 | —                 |
| <b>ppp</b>          | PPP traffic                                                              | X                                                 | —                 |
| <b>pppoe</b>        | PPPoE traffic                                                            | X                                                 | —                 |
| <b>proto-802-1x</b> | 802.1X traffic                                                           | —                                                 | X                 |
| <b>ptp</b>          | PTP traffic                                                              | X                                                 | X                 |
| <b>pvstp</b>        | PVSTP traffic                                                            | X                                                 | X                 |
| <b>radius</b>       | RADIUS traffic                                                           | X                                                 | X                 |
| <b>re-services</b>  | Captive portal content delivery traffic for Routing Engine HTTP redirect | X                                                 | —                 |
| <b>redirect</b>     | Traffic that triggers ICMP redirects                                     | X                                                 | —                 |
| <b>reject</b>       | Packets rejected by a next-hop forwarding decision                       | X                                                 | X                 |
| <b>rejectv6</b>     | IPv6 packets rejected by a next-hop forwarding decision                  | X                                                 | —                 |

Table 22: Supported Protocol Groups (*continued*)

| Protocol Group         | Description                                                                                             | MX Series Routers, T4000 Routers, EX9200 Switches | QFX10000 Switches |
|------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------|-------------------|
| <b>resolve</b>         | Unclassified IPv4 and IPv6 resolve packets sent to the host because of a traffic request resolve action | X                                                 | X                 |
| <b>rip</b>             | RIP traffic                                                                                             | X                                                 | X                 |
| <b>ripv6</b>           | RIPv6 traffic                                                                                           | X                                                 | —                 |
| <b>rsvp</b>            | RSVP traffic                                                                                            | X                                                 | X                 |
| <b>rsvpv6</b>          | RSVPv6 traffic                                                                                          | X                                                 | —                 |
| <b>snmp</b>            | SNMP traffic                                                                                            | X                                                 | X                 |
| <b>snmpv6</b>          | SNMPv6 traffic                                                                                          | X                                                 | —                 |
| <b>ssh</b>             | SSH traffic                                                                                             | X                                                 | X                 |
| <b>sshv6</b>           | SSHv6 traffic                                                                                           | X                                                 | —                 |
| <b>stp</b>             | STP traffic                                                                                             | X                                                 | X                 |
| <b>syslog</b>          | System log messages UDP traffic on port 6333 for the Routing Engine syslog server                       | X                                                 | —                 |
| <b>tacacs</b>          | TACACS+ traffic                                                                                         | --                                                | X                 |
| <b>tcp-flags</b>       | Traffic with TCP flags                                                                                  | X                                                 | —                 |
| <b>telnet</b>          | Telnet traffic                                                                                          | X                                                 | X                 |
| <b>telnetv6</b>        | Telnetv6 traffic                                                                                        | X                                                 | —                 |
| <b>ttl</b>             | Time to Live packets                                                                                    | X                                                 | X                 |
| <b>tunnel-fragment</b> | Tunnel fragments traffic                                                                                | X                                                 | —                 |
| <b>unclassified</b>    | Unclassified traffic                                                                                    | X                                                 | —                 |
| <b>virtual-chassis</b> | Virtual chassis traffic                                                                                 | X                                                 | —                 |
| <b>vrrp</b>            | VRRP traffic                                                                                            | X                                                 | X                 |
| <b>vrrpv6</b>          | VRRPv6 traffic                                                                                          | X                                                 | —                 |

**Required Privilege Level** view

- Related Documentation**
- [clear ddos-protection protocols on page 232](#)
  - [show ddos-protection protocols culprit-flows](#)
  - [show ddos-protection protocols flow-detection](#)
  - [show ddos-protection protocols parameters on page 253](#)
  - [show ddos-protection protocols statistics on page 260](#)
  - [show ddos-protection protocols violations on page 273](#)

**List of Sample Output** [show ddos-protection protocols on page 248](#)  
[show ddos-protection protocols \(Specific Packet Type with Flow Detection Disabled\) on page 250](#)  
[show ddos-protection protocols \(Specific Packet Type with Flow Detection Enabled and Automatic\) on page 250](#)  
[show ddos-protection protocols \(Specific Packet Type with Bandwidth Violation\) on page 251](#)

**Output Fields** [Table 23 on page 244](#) lists the output fields for the **show ddos-protection protocols** command. Output fields are listed in the approximate order in which they appear.

**Table 23: show ddos-protection protocols Output Fields**

| Field Name              | Field Description                                                                                             |
|-------------------------|---------------------------------------------------------------------------------------------------------------|
| Packet types            | Number of packet types                                                                                        |
| Modified                | Number of packets for which policer values have been modified from the default.                               |
| Received traffic        | Number of traffic flows received.                                                                             |
| Currently violated      | Number of flows that are currently violating the flow bandwidth limit.                                        |
| Currently tracked flows | Number of active flows that are being tracked as culprit flows by flow detection.                             |
| Total detected flows    | Total number of culprit flows that have been detected, including those that have recovered or timed out.      |
| Protocol Group          | Name of protocol group.                                                                                       |
| Packet type             | Name of packet type in protocol group.                                                                        |
| Bandwidth               | Bandwidth policer value; number of packets per second that is allowed before a violation is declared.         |
| Burst                   | Burst policer value; the maximum number of packets that is allowed in a burst before a violation is declared. |



Table 23: show ddos-protection protocols Output Fields (*continued*)

| Field Name                   | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Priority                     | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Recover time                 | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Enabled                      | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Bypass aggregate             | State of the bypass aggregate configuration: <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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Flow detection configuration | State of flow detection configured on the router: <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 23: 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 23: 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> <p><b>NOTE:</b> On MX Series routers with built-in MPCs—the MX5, MX10, MX40, MX80, and MX104 routers—this field actually displays information for tfeb0 because these routers have no Flexible PIC Concentrator (FPC) slots. Instead, the Packet Forwarding Engine has two “pseudo” FPCs (FPC 0 and FPC1).</p> |
| <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: Bwidth (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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Table 23: show ddos-protection protocols Output Fields (*continued*)

| Field Name      | Field Description                                                                                                                                                                                             |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Log flow</b> | State of automatic logging of suspicious traffic flows for the packet type: on (Yes) or off (No).                                                                                                             |
| <b>Time out</b> | State of culprit flow timeout behavior for the packet type: flow is suppressed or monitored for a configured timeout period (Yes) or flow is suppressed or monitored until it is no longer in violation (No). |

## 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>      | <p>Command introduced in Junos OS Release 11.2.</p> <p>Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <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.</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 232</a></li> <li><a href="#">show ddos-protection protocols on page 234</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 260</a></li> <li><a href="#">show ddos-protection protocols violations on page 273</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection protocols parameters on page 255</a><br><a href="#">show ddos-protection protocols parameters brief on page 256</a><br><a href="#">show ddos-protection protocols dhcpv4 parameters brief on page 257</a><br><a href="#">show ddos-protection protocols dhcpv4 parameters terse on page 258</a><br><a href="#">show ddos-protection protocols dhcpv4 parameters on page 258</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Output Fields** Table 24 on page 254 lists the output fields for the **show ddos-protection protocols parameters** command. Output fields are listed in the approximate order in which they appear.

**Table 24: 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.                                                                                                                                              | 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.                                                                                                                                                                                                         | <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 24: 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.  | <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 |
| dhcpv4 | aggregate  | 669*  | 5000  | medium | 300 | yes    | -- | no |
| dhcpv4 | 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 |
| ...    |            |       |       |        |     |        |    |    |
| 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 dhcpv4 parameters brief

```

user@host> show ddos-protection protocols dhcpv4 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
dhcpv4 aggregate 669* 5000 medium 300 yes -- no
dhcpv4 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>                   | <b>show ddos-protection protocols &lt;protocol-group&gt; statistics</b><br><b>&lt;brief   detail   terse&gt;</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b>      | <p>Command introduced in Junos OS Release 11.2.</p> <p>Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <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.</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 232</a></li> <li><a href="#">show ddos-protection protocols on page 234</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 parameters on page 253</a></li> <li><a href="#">show ddos-protection protocols violations on page 273</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection protocols statistics on page 262</a><br><a href="#">show ddos-protection protocols statistics brief on page 265</a><br><a href="#">show ddos-protection protocols statistics terse on page 266</a><br><a href="#">show ddos-protection protocols pppoe statistics on page 267</a><br><a href="#">show ddos-protection protocols pppoe statistics brief on page 269</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Output Fields</b>            | Table 25 on page 261 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 25: 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | All levels      |
| <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>                                                                                                                                                                | detail none     |
| <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> | detail none     |

Table 25: 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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <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-unclass   | aggregate   | 0                  | 0                 | 0          | 0                | ok    |
| ipv6-unclass   | 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 Packet Received Dropped Rate Violation State
group type (packets) (packets) (pps) counts
ipv4-unc1s 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 |
| m1p        | aggregate | 624774  | 0      | 0 | 0 | ok |
| m1p        | 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 |
| unc1s      | 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<br>group | Packet<br>type | Received<br>(packets) | Dropped<br>(packets) | Rate<br>(pps) | Violation<br>counts | State |
|-------------------|----------------|-----------------------|----------------------|---------------|---------------------|-------|
| 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>      | <p>Command introduced in Junos OS Release 11.2.</p> <p>Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p> |
| <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 232</a></li> <li>• <a href="#">show ddos-protection protocols on page 234</a></li> <li>• <a href="#">show ddos-protection version on page 272</a></li> </ul>                                                 |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection statistics on page 271</a>                                                                                                                                                                                                                                               |
| <b>Output Fields</b>            | <a href="#">Table 26 on page 270</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 26: show ddos-protection statistics Output Fields**

| Field Name                        | Field Description                                                                                 |
|-----------------------------------|---------------------------------------------------------------------------------------------------|
| Policing on routing engine        | Shows whether or not policing is enabled on the Routing Engine.                                   |
| Policing on FPC                   | Shows whether or not policing is enabled on the line card.                                        |
| Flow detection                    | Shows whether or not flow detection is enabled.                                                   |
| Logging                           | Shows whether or not DDoS event logging is enabled.                                               |
| Policer violation report rate     | Shows the violation report rate as a percentage.                                                  |
| Flow report rate                  | Shows the flow report rate as a percentage.                                                       |
| 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. |

Table 26: show ddos-protection statistics Output Fields (*continued*)

| Field Name             | Field Description                     |
|------------------------|---------------------------------------|
| Total violation counts | Total number of bandwidth violations. |

## Sample Output

### show ddos-protection statistics

```
user@host> show ddos-protection statistics
DDOS protection global statistics:

 Policing on routing engine: Yes
 Policing on FPC: Yes
 Flow detection: No
 Logging: Yes
 Policer violation report rate: 100
 Flow report rate: 100
 Currently violated packet types: 2
 Packet types have seen violations: 2
 Total violation counts: 2
 Currently tracked flows: 0
 Total detected flows: 0
```

## show ddos-protection version

|                                 |                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show ddos-protection version</b>                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | <p>Command introduced in Junos OS Release 11.2.</p> <p>Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p> |
| <b>Description</b>              | Display the DDoS protection version and the total numbers of protocol groups and packet types that this version can be configured in this version.                                                                                                                                                        |
| <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 232</a></li> <li>• <a href="#">show ddos-protection protocols on page 234</a></li> <li>• <a href="#">show ddos-protection statistics on page 270</a></li> </ul>                                              |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection version on page 272</a>                                                                                                                                                                                                                                                  |
| <b>Output Fields</b>            | Table 27 on page 272 lists the output fields for the <b>show ddos-protection version</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                 |

Table 27: show ddos-protection version Output Fields

| Field Name                        | Field Description                                                |
|-----------------------------------|------------------------------------------------------------------|
| <b>Version</b>                    | Version number of the DDoS protection code.                      |
| <b>Total protocol groups</b>      | Number of protocol groups configured with DDoS protection.       |
| <b>Total tracked packet types</b> | Number of protocol packet types configured with DDoS protection. |

## 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

```

## show ddos-protection protocols violations

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show ddos-protection protocols &lt;protocol-group&gt; violations</b>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | <p>Command introduced in Junos OS Release 11.2.</p> <p>Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>                                                                                                                                                                                                |
| <b>Description</b>              | Display information about DDoS policer violations 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>protocol-group</b>—(Optional) Name of a particular protocol group. See <a href="#">show ddos-protection protocols</a> for a list of available groups.</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 232</a></li> <li>• <a href="#">show ddos-protection protocols on page 234</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 parameters on page 253</a></li> <li>• <a href="#">show ddos-protection protocols statistics on page 260</a></li> </ul> |
| <b>List of Sample Output</b>    | <p><a href="#">show ddos-protection protocols violations on page 274</a></p> <p><a href="#">show ddos-protection protocols lldp violations on page 274</a></p> <p><a href="#">show ddos-protection protocols pppoe violations on page 274</a></p>                                                                                                                                                                                                                                                        |
| <b>Output Fields</b>            | Table 28 on page 273 lists the output fields for the <b>show ddos-protection protocols violations</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                   |

**Table 28: show ddos-protection protocols violations Output Fields**

| Field Name                                     | Field Description                                                                      |
|------------------------------------------------|----------------------------------------------------------------------------------------|
| Number of packet types that are being violated | Number of individual policers and aggregate policers that are currently being violated |
| Protocol Group                                 | Name of protocol group                                                                 |
| Packet type                                    | Name of packet type in protocol group                                                  |
| Bandwidth (pps)                                | Policer bandwidth                                                                      |

**Table 28: show ddos-protection protocols violations Output Fields (continued)**

| Field Name                                     | Field Description                                                                  |
|------------------------------------------------|------------------------------------------------------------------------------------|
| <b>Arrival rate (pps)</b>                      | Current traffic rate for packets arriving from all cards and at the Routing Engine |
| <b>Peak rate (pps)</b>                         | Highest traffic rate for packets arriving from all cards and at the Routing Engine |
| <b>Policer bandwidth violation detected at</b> | Timestamp of the policer violation                                                 |
| <b>Detected on</b>                             | Slot number of the card on which the violation was detected                        |

## Sample Output

### show ddos-protection protocols violations

```

user@host> show ddos-protection protocols violations
Number of packet types that are being violated: 2
Protocol Packet Bandwidth Arrival Peak Policer bandwidth
group type (pps) rate(pps) rate(pps) violation detected at
pppoe padi 500 2000 2001 2011-04-19 08:23:17 PDT
 Detected on: FPC-1
pppoe padr 500 1999 2001 2011-04-19 08:23:17 PDT
 Detected on: FPC-1

```

### show ddos-protection protocols lldp violations

```

user@host> show ddos-protection protocols lldp violations
Number of packet types that are being violated: 0

```

### show ddos-protection protocols pppoe violations

```

user@host> show ddos-protection protocols pppoe violations
Number of packet types that are being violated: 2
Protocol Packet Bandwidth Arrival Peak Policer bandwidth
group type (pps) rate(pps) rate(pps) violation detected at
pppoe padi 500 2000 2001 2011-04-19 08:23:17 PDT
 Detected on: FPC-1
pppoe padr 500 1999 2001 2011-04-19 08:23:17 PDT
 Detected on: FPC-1

```