



Junos[®] OS

Distributed Denial-of-Service Protection Feature Guide

Release
13.2



Published: 2013-07-25

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

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

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

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

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

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

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

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

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

Junos® OS Distributed Denial-of-Service Protection Feature Guide

13.2

Copyright © 2013, 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	xi
	Documentation and Release Notes	xi
	Supported Platforms	xi
	Using the Examples in This Manual	xi
	Merging a Full Example	xii
	Merging a Snippet	xii
	Documentation Conventions	xiii
	Documentation Feedback	xv
	Requesting Technical Support	xv
	Self-Help Online Tools and Resources	xv
	Opening a Case with JTAC	xvi
Part 1	Overview	
Chapter 1	Distributed Denial-of-Service Protection	3
	Distributed Denial-of-Service (DDoS) Protection Overview	3
	Policer Types and Packet Priorities	4
	Example of Policer Priority Behavior	4
	Policer Hierarchy	5
	Example of Policer Bandwidth Limit Behavior	7
Chapter 2	Flow Detection in Subscriber Access Networks	9
	DDoS Protection Flow Detection Overview	9
	Flow Detection and Control	9
	Flow Tracking	10
	Notifications	10
Part 2	Configuration	
Chapter 3	Configuration Overview for DDoS	15
	Configuring Protection Against DDoS Attacks	15
Chapter 4	Configuration Tasks for DDoS	17
	Configuring DDoS Protection Policers for Individual Packet Types	17
	Disabling DDoS Protection Policers and Logging Globally	21
Chapter 5	Example	23
	Example: Configuring DDoS Protection	23
Chapter 6	Configuration Overview for Flow Detection	33
	Configuring Flow Detection for DDoS Protection	33

Chapter 7	Configuration Tasks for Flow Detection	35
	Configuring Flow Detection for DDoS Protection	35
	Enabling Flow Detection for All Protocol Groups and Packet Types	37
	Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types	37
	Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types	37
	Configuring the Detection Period for Suspicious Flows	38
	Configuring the Recovery Period for a Culprit Flow	38
	Configuring the Timeout Period for a Culprit Flow	39
	Configuring Flow Detection for Individual Protocol Groups or Packets	40
	Configuring How Flow Detection Operates at Each Flow Aggregation Level	40
	Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level	42
	Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level	42
	Disabling Automatic Logging of Culprit Flow Events for a Packet Type	43
Chapter 8	Configuration Statements	45
	[edit system ddos-protection] Hierarchy Level	45
	bandwidth (DDoS)	46
	bandwidth-scale (DDoS)	47
	burst (DDoS)	47
	burst-scale (DDoS)	48
	bypass-aggregate (DDoS)	48
	ddos-protection (DDoS)	49
	disable-fpc (DDoS)	50
	disable-logging (DDoS)	51
	disable-routing-engine (DDoS)	51
	flow-detection (DDoS Flow Detection)	52
	flow-detection (DDoS Packet Level)	53
	flow-detection-mode (DDoS Flow Detection)	54
	flow-detect-time (DDoS Flow Detection)	55
	flow-level-bandwidth (DDoS Flow Detection)	56
	flow-level-control (DDoS Flow Detection)	56
	flow-level-detection (DDoS Flow Detection)	57
	flow-recover-time (DDoS Flow Detection)	58
	flow-report-rate (DDoS Flow Detection)	58
	flow-timeout-time (DDoS Flow Detection)	59
	fpc (DDoS)	59
	global (DDoS)	60
	logical-interface (DDoS Flow Detection)	61
	no-flow-logging (DDoS Flow Detection)	62
	physical-interface (DDoS Flow Detection)	63
	priority (DDoS)	64
	protocols (DDoS)	65
	recover-time (DDoS)	73
	subscriber (DDoS Flow Detection)	74
	timeout-active-flows (DDoS Flow Detection)	75
	traceoptions (DDoS)	76

	violation-report-rate (DDoS Flow Detection)	78
Part 3	Administration	
Chapter 9	Verifying and Monitoring Configurations	81
	Verifying and Managing DDoS Protection	81
	Verifying and Managing Flow Detection	82
Chapter 10	Monitoring Commands	83
	clear ddos-protection protocols	84
	show ddos-protection protocols	85
	show ddos-protection protocols culprit-flows	101
	show ddos-protection protocols flow-detection	104
	show ddos-protection protocols parameters	108
	show ddos-protection protocols statistics	115
	show ddos-protection protocols violations	126
	show ddos-protection statistics	128
	show ddos-protection version	129
Part 4	Troubleshooting	
Chapter 11	Acquiring Troubleshooting Information	133
	Tracing DDoS Protection Operations	133
	Configuring the DDoS Protection Trace Log Filename	134
	Configuring the Number and Size of DDoS Protection Log Files	134
	Configuring Access to the DDoS Protection Log File	135
	Configuring a Regular Expression for DDoS Protection Messages to Be Logged	135
	Configuring the DDoS Protection Tracing Flags	136
	Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged	136
	Collecting Subscriber Access Logs Before Contacting Juniper Technical Support	136
Chapter 12	Troubleshooting Configuration Statements	139
	traceoptions (DDoS)	140
Part 5	Index	
	Index	145

List of Figures

Part 1	Overview	
Chapter 1	Distributed Denial-of-Service Protection	3
	Figure 1: Policer Hierarchy for PPPoE Packets	5
	Figure 2: Policer Hierarchy for DHCPv4 Packets	6

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xiii
	Table 2: Text and Syntax Conventions	xiii
Part 1	Overview	
Chapter 2	Flow Detection in Subscriber Access Networks	9
	Table 3: Triggering Event for Flow Detection Reports	11
	Table 4: Triggering Event for Bandwidth Violation Reports	11
Part 3	Administration	
Chapter 10	Monitoring Commands	83
	Table 5: show ddos-protection protocols Output Fields	92
	Table 6: show ddos-protection protocols culprit-flows Output Fields	101
	Table 7: show ddos-protection protocols flow-detection Output Fields	104
	Table 8: show ddos-protection protocols parameters Output Fields	109
	Table 9: show ddos-protection protocols statistics Output Fields	116
	Table 10: show ddos-protection protocols violations Output Fields	126
	Table 11: show ddos-protection statistics Output Fields	128
	Table 12: show ddos-protection version Output Fields	129

About the Documentation

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

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:

- MX Series
- T4000

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 xiii 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.

Table 2 on page xiii 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
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active

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

Convention	Description	Examples
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
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)	Enclose 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 <i>(string1 string2 string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identify 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.
> (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 send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release 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 JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>

- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

- [Distributed Denial-of-Service Protection on page 3](#)
- [Flow Detection in Subscriber Access Networks on page 9](#)

CHAPTER 1

Distributed Denial-of-Service Protection

- [Distributed Denial-of-Service \(DDoS\) Protection Overview on page 3](#)

Distributed Denial-of-Service (DDoS) Protection Overview

A denial-of-service 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 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's control plane. This results in an excessive processing load that disrupts normal network operations.

Junos OS DDoS protection enables the router to continue functioning while under an 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. Protection and monitoring persists across graceful Routing Engine switchover (GRES) and unified in-service-software-upgrade (ISSU) switchovers. Protection is not diminished as the number of subscribers increases.

To protect against DDoS attacks, you can configure policers for host-bound exception traffic. The policers specify rate limits for individual types of protocol control packets or for all control packet types for a protocol. You can monitor policer actions for packet types and protocol groups at the level of the router, Routing Engine, and line cards. You can also control logging of policer events.

The policers at the MPC or FPC5 are the first line of protection. Control traffic is dropped when it exceeds any configured policer values or, for unconfigured policers, the default policer values. Each violation 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.

Policer states and statistics from each line card are relayed to the Routing Engine and aggregated. The policer states are maintained during a switchover. Although line card statistics and violation counts are preserved during a switchover, Routing Engine policer statistics are not.



NOTE: DDoS protection is supported only on MX Series routers that have only MPCs installed and T4000 routers that have only FPC5s installed. If the router has other line cards in addition to MPCs or FPC5s, respectively, the CLI accepts the configuration but the other line cards are not protected and so the router is not protected.

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 PPPoE control packet types or to all DHCPv4 control packet types. You can specify bandwidth and burst limits, scale the bandwidth and burst limits, and set a traffic priority 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 each control packet type within a protocol group. For example, you can configure a policer for one or more types of PPPoE control packets. You can specify bandwidth and burst limits, scale the bandwidth and burst limits, and set a traffic priority for packet-type policers. 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- 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- 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

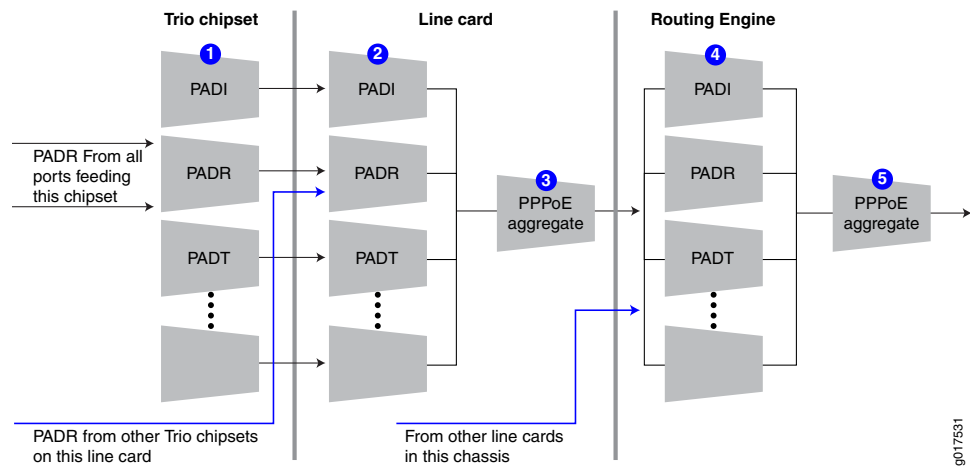
For example, consider how you might configure packet types within the PPPoE protocol group. Ignoring other PPPoE packet types for this example, suppose you configure individual policers for PADI and PADT packets, as well as a PPPoE aggregate policer for all those packets. PADT packets are more important than PADI packets, because PADT packets enable the PPPoE application to release resources to accept new connections. Therefore, you might assign high priority to the PADT packets and low priority to the PADI packets.

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

Policer Hierarchy

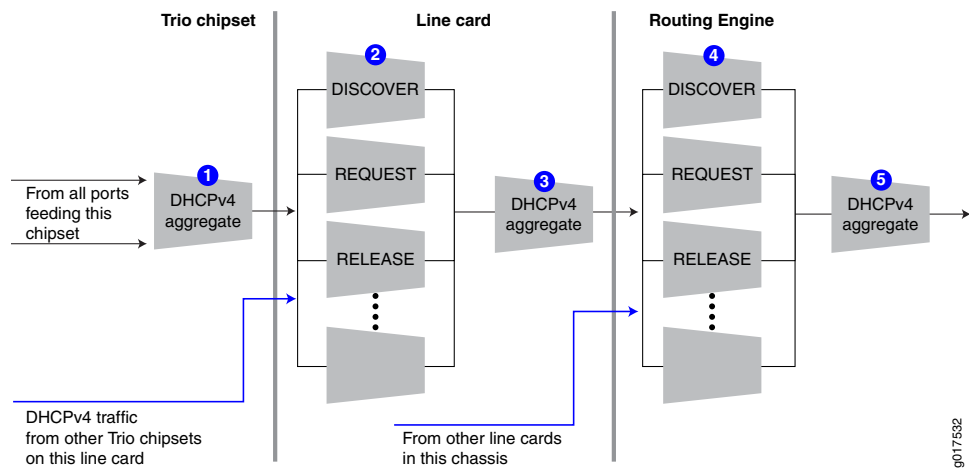
DDoS policers are organized to match the hierarchical flow of protocol control traffic. Control traffic arriving from all ports of a line card converges on the card's Packet Forwarding Engine. Control traffic from all line cards on the router converges on the Routing Engine. Similarly, the DDoS policers are placed hierarchically along the control paths so that excess packets are dropped as early as possible on the path. This design preserves system resources by removing excess, malicious traffic so that the Routing Engine receives only the amount of traffic that it can process. To implement this design, five DDoS policers are present: One at the chipset, two at the line card, and two at the Routing Engine. [Figure 1 on page 5](#) shows the policer process for PPPoE traffic. [Figure 2 on page 6](#) shows the policer process for DHCPv4 traffic. (The same process applies to DHCPv6 traffic.)

Figure 1: Policer Hierarchy for PPPoE Packets



g07531

Figure 2: Policer Hierarchy for DHCPv4 Packets



Control packets arrive at the chipset on the MPC or FPC5 for processing and forwarding. The first policer (1) is either an individual policer ([Figure 1 on page 5](#)) or an aggregate policer ([Figure 2 on page 6](#)).

- The first policer is an individual policer for protocol groups that support individual policers, with two exceptions. For DHCPv4 and DHCPv6 traffic, the first policer is an aggregate policer.
- The first policer is an aggregate policer for protocol groups that support only aggregate policers.

Traffic that passes the first policer is monitored by one or both of the line card policers. If the card has more than one chipset, traffic from all chipsets converges on the line card policers.

- When the traffic belongs to a protocol group that supports individual policers, it passes through the line card individual policer (2) and then the line card aggregate policer (3). Traffic that passes the individual policer can be dropped by the aggregate policer. Although DHCPv4 and DHCPv6 traffic was monitored by an aggregate policer at the chipset, at the line card it is handled like other protocols that support individual policers.
- When the traffic belongs to a protocol group that supports only aggregate policers, only the line card aggregate policer monitors the traffic.

Traffic that passes the line card policers is monitored by one or both of the Routing Engine policers. Traffic from all MPCs or FPC5s converges on the Routing Engine policers.

- When the traffic belongs to a protocol group that supports individual policers, it passes through the Routing Engine individual policer (4) and then the Routing Engine aggregate policer (5). Traffic that passes the individual policer can be dropped by the aggregate policer. As it was at the line card level, DHCPv4 and DHCPv6 traffic at the Routing Engine is handled like other protocols that support individual policers.
- When the traffic belongs to a protocol group that supports only aggregate policers, only the aggregate policer monitors the traffic.

The result of this design is that traffic for protocol groups that support only aggregate policers is evaluated by three policers. Among other groups, this includes ANCP, dynamic VLAN, FTP, and IGMP traffic. Traffic for protocol groups that support both aggregate and individual policers is evaluated by all five policers. Among other groups, this includes DHCPv4, MLP, PPP, PPPoE, and virtual chassis traffic.

Figure 1 on page 5 shows how DDoS protection polices PPPoE control packets:

1. PADR packets, for example, are evaluated at the first policer on the chipset to determine whether they are within the bandwidth limits. PADR packets that exceed the limit are dropped.
2. All PADR packets that pass the policer on all chipsets on the MPC or FPC5 are next evaluated by the line card individual policer. PADR packets that exceed the limit are dropped.
3. All PADR packets that pass the line card individual policer proceed to the line card aggregate policer. PADR packets that exceed the limit are dropped.
4. All PADR packets that are passed by the line card aggregate policers on all MPCs or FPC5s on the router proceed to the Routing Engine individual policer. PADR packets that exceed the limit are dropped.
5. Finally, all PADR packets that are passed by the Routing Engine individual policer proceed to the Routing Engine aggregate policer. PADR packets that exceed the limit are dropped. PADR packets that are not dropped here are passed along as safe, normal traffic.

By default, all three individual policers (chipset, line card, and Routing Engine) have the same bandwidth limit for a given packet type. This design enables all the control traffic from a chipset and line card to reach the Routing engine, as long as there is no competing traffic of the same type from other chipsets or line cards. When competing traffic is present, excess packets are dropped at the convergence points. That is, they are dropped at the line card for all competing chipsets and at the Routing Engine for all competing line cards.

Example of Policer Bandwidth Limit Behavior

For example, suppose you set the policer bandwidth for PADI packets to 1000 packets per second. This value applies to the individual PADI policers at the chipset, the line card, and the Routing Engine. If only the card in slot 5 is receiving PADI packets, then up to 1000 PADI pps can reach the Routing Engine (if the PPPoE aggregate policer is not exceeded). However, suppose the card in slot 9 is also receiving PADI packets at 1000 pps and that its PPPoE aggregate policer is not exceeded. The traffic passes the individual and aggregate policers at both line cards and proceeds to the Routing Engine. At the Routing Engine, the combined bandwidth is 2000 pps. Because the PADI policer at the Routing Engine allows only 1000 PADI pps to pass, it drops the excess 1000 packets. It continues to drop the excess packets for as long as the bandwidth is exceeded.

You can apply a scaling factor for both the bandwidth limit and the burst limit at the line card. This enables you to fine-tune the traffic limits for each slot. For example, suppose the individual policer sets the PADI packet bandwidth to 1000 pps and the burst size to 50,000 packets. You can reduce the traffic limit for PADI packets on any line card by

specifying the slot number and scaling factor. A bandwidth scaling factor of 20 for slot 5 reduces the traffic in this example to 20 percent of 1000 pps, or 200 pps for the line card in that slot. Similarly, a burst scaling factor of 50 for that slot reduces the burst size by 50 percent to 25,000 packets. By default, scaling factors are set to 100 so traffic can pass through at 100 percent of the rate limit.

**Related
Documentation**

- [Configuring Protection Against DDoS Attacks on page 15](#)
- [DDoS Protection Flow Detection Overview on page 9](#)

CHAPTER 2

Flow Detection in Subscriber Access Networks

- [DDoS Protection Flow Detection Overview on page 9](#)

DDoS Protection Flow Detection Overview

Flow detection is an enhancement to DDoS protection that supplements the DDoS policer hierarchies; it is part of a complete DDOS protection solution. Flow detection uses a limited amount of hardware resources to monitor the arrival rate of host-bound flows of control traffic. Flow detection is much more scalable than a solution based on filter policers. Filter policers track all flows, which consumes a considerable amount of resources. In contrast, flow detection only tracks flows it identifies as suspicious, using far fewer resources to do so.

The flow detection application has two interrelated components, detection and tracking. Detection is the process where flows suspected of being improper are identified and subsequently controlled. Tracking is the process where flows are tracked to determine whether they are truly hostile and when these flows recover to within acceptable limits.

- [Flow Detection and Control on page 9](#)
- [Flow Tracking on page 10](#)
- [Notifications on page 10](#)

Flow Detection and Control

Flow detection is disabled by default. When you enable it at the **[edit system ddos-protection global]** hierarchy level, the application begins monitoring control traffic flows when a DDoS protection policer is violated for all protocol groups and packet types. Other than event report rates, all other characteristics of flow detection are configurable only at the level of individual packet types.

Control flows are aggregated at three levels. The *subscriber level* is the finest grained of the three and consists of flows for individual subscriber sessions. The *logical interface level* aggregates multiple subscriber flows, so it is coarser grained and does not provide discrimination into individual subscriber flows. The *physical interface level* aggregates multiple logical interface flows, so it provides the coarsest view of traffic flows.

You can turn flow detection off or on at any of these levels. You can also configure whether it is automatically triggered by the violation of a DDoS protection policer or is always on—meaning that it always monitors flows, even when no policer is being violated. Flow detection begins at the finest-grained level that has detection configured to **on** or **automatic**.

When a flow arrives, flow detection checks whether the flow is already listed in a table of *suspicious* flows. A suspicious flow is one that exceeds the bandwidth allowed by default or configuration. If the flow is not in the table and the aggregation level flow detection mode is **on**, then flow detection lists the flow in the table. If the flow is not in the table and the flow detection mode is **automatic**, flow detection checks whether this flow is suspicious.

If the flow is suspicious, then it goes in the flow table. If the flow is not suspicious, then it is processed the same way at the next coarser aggregation level that has flow detection set to **on**. If none of the higher levels have detection on, then the flow continues to the DDoS protection packet policer for action, where it can be passed or dropped.

When the initial check finds the flow in the table, then the flow is dropped, policed, or kept, depending on the control mode setting for that aggregation level. All packets in dropped flows are dropped. In policed flows, packets are dropped until the flow is within the acceptable bandwidth for the aggregation level. Kept flows are passed along to the next aggregation level for processing.

Flow Tracking

The flow detection application tracks flows that have been listed in the suspicious flow table. It periodically checks each entry in the table to determine whether the listed flow is still suspicious (violating the bandwidth). If a suspicious flow has continuously violated the bandwidth since it was inserted in the table for a period greater than the configurable flow detection period, then it is considered to be a *culprit* flow rather than merely suspicious. However, if the bandwidth has been violated for less than the detection period, the violation is treated as a false positive. Flow detection considers the flow to be safe and stops tracking it (deletes it from the table).

You can enable a timeout feature that suppresses culprit flows for a configurable timeout period, during which the flow is kept in the flow table. (Suppression is the default behavior, but the flow detection action can be changed by the flow level control configuration.) If the check of listed flows finds one for which the timeout is enabled and the timeout period has expired, then the flow has timed out and it is removed from the flow table.

If the timeout has not yet expired or if the timeout feature is not enabled, then the application performs a recovery check. If the time since the flow last violated the bandwidth is longer than the configurable recovery period, the flow has recovered and is removed from the flow table. If the time since last violation is less than the recovery period, the flow is kept in the flow table.

Notifications

By default, flow detection automatically generates system logs for a variety of events that occur during flow detection. The logs are referred to as *reports* in the flow detection

CLI. All protocol groups and packet types are covered by default, but you can disable automatic logging for individual packet types. You can also configure the rate at which reports are sent, but this applies globally to all packet types.

Each report belongs to one of the following two types:

- Flow reports—These reports are generated by events associated with the identification and tracking of culprit flows. Each report includes identifying information for the flow that experienced the event. This information is used to accurately maintain the flow table; flows are deleted or retained in the table based on the information in the report. [Table 3 on page 11](#) describes the event that triggers each flow report.

Table 3: Triggering Event for Flow Detection Reports

Name	Description
DDOS_SCFD_FLOW_FOUND	A suspicious flow is detected.
DDOS_SCFD_FLOW_TIMEOUT	The timeout period expires for a culprit flow. Flow detection stops suppressing (or monitoring) the flow.
DDOS_SCFD_FLOW_RETURN_NORMAL	A culprit flow returns to within the bandwidth limit.
DDOS_SCFD_FLOW_CLEARED	A culprit flow is cleared manually with a clear command or automatically as the result of suspicious flow monitoring shifting to a different aggregation level.
DDOS_SCFD_FLOW_AGGREGATED	Control flows are aggregated to a coarser level. This event happens when the flow table nears capacity or when the flow cannot be found at a particular flow level and the next coarser level has to be searched.
DDOS_SCFD_FLOW_DEAGGREGATED	Control flows are deaggregated to a finer level. This event happens when the flow table is not very full or when flow control is effective and the total arrival rate for the flow at the policer for the packet type is below its bandwidth for a fixed, internal period.

- Bandwidth violation reports—These reports are generated by events associated with the discovery of suspicious flows. Each report includes identifying information for the flow that experienced the event. This information is used to track the suspicious flow and identify flows that are placed in the flow table. [Table 4 on page 11](#) describes the event that triggers each violation report.

Table 4: Triggering Event for Bandwidth Violation Reports

Name	Description
DDOS_PROTOCOL_VIOLATION_SET	The incoming traffic for a violated control protocol returned to normal.
DDOS_PROTOCOL_VIOLATION_CLEAR	The incoming traffic for a control protocol exceeded the configured bandwidth.

A report is sent only when triggered by an event; that is, there are no null or empty reports. Because the reports are made periodically, the only events of interest are ones that occur during the interval since the last report.

- Related Documentation**
- [Configuring Flow Detection for DDoS Protection on page 33](#)

PART 2

Configuration

- [Configuration Overview for DDoS on page 15](#)
- [Configuration Tasks for DDoS on page 17](#)
- [Example on page 23](#)
- [Configuration Overview for Flow Detection on page 33](#)
- [Configuration Tasks for Flow Detection on page 35](#)
- [Configuration Statements on page 45](#)

CHAPTER 3

Configuration Overview for DDoS

- [Configuring Protection Against DDoS Attacks on page 15](#)

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 and T4000 routers that have only FPC5s installed. If the router has other line cards in addition to MPCs or FPC5s, respectively, the CLI accepts the configuration but the other line cards are not protected and so the router is not protected.

To configure DDoS protection:

1. (Optional) Configure global DDoS settings.
See [“Disabling DDoS Protection Policers and Logging Globally” on page 21](#).
2. (Optional) Configure DDoS settings for individual packet types.
See [“Configuring DDoS Protection Policers for Individual Packet Types” on page 17](#).
3. (Optional) Configure tracing for DDoS operations.
See [“Tracing DDoS Protection Operations” on page 133](#).

Related Documentation

- [Distributed Denial-of-Service \(DDoS\) Protection Overview on page 3](#)
- [Example: Configuring DDoS Protection on page 23](#)

CHAPTER 4

Configuration Tasks for DDoS

- [Configuring DDoS Protection Policers for Individual Packet Types on page 17](#)
- [Disabling DDoS Protection Policers and Logging Globally on page 21](#)

Configuring DDoS Protection Policers for Individual Packet Types

DDoS policers are applied to control packet traffic. You configure the maximum allowed traffic rate, maximum burst size, traffic priority, and how much time must pass since the last violation before the traffic flow is considered to have recovered from the attack. You can also scale the bandwidth and burst values for individual line cards so that the policers at this level trigger at lower thresholds than the overall protocol or packet thresholds.

You can configure an aggregate policer for any protocol group. The aggregate policer applies to the combination of all types of control packet traffic for that group. When you configure an aggregate policer for certain protocol groups, you can optionally bypass that policer for one or more particular packet types in that group. For those same groups, you can configure policers for individual packet types instead of configuring an aggregate policer.

DDoS protection is enabled by default. Although all policers have default parameter values, these values might not accurately reflect the control traffic pattern of your network.



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 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 dhcpv4 parameters brief` command.

You can disable a packet type's policer at either the Routing Engine, at a specified line card, or for all line cards. You can also disable logging of all DDoS events for individual packet types within a protocol group.

To configure individual, packet-level DDoS settings:

1. Specify the protocol group.

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

For example, to specify the DHCPv4 protocol group:

```
[edit system ddos-protection protocols]
user@host# edit dhcpv4
```

2. Specify the packet type or the combination of all packet types in the group.

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

or

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

For example, to specify the DHCPv4 release packets:

```
[edit system ddos-protection protocols dhcpv4]
user@host# edit release
```

3. (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 600 packets per second for DHCPv4 release packets:

```
[edit system ddos-protection protocols dhcpv4 release]
user@host# set bandwidth 600
```

4. (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 5000 DHCPv4 release packets:

```
[edit system ddos-protection protocols dhcpv4 release]
user@host# set burst 5000
```

5. (Optional) Set the traffic priority.

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

For example, to specify a medium priority for DHCPv4 release packets:

```
[edit system ddos-protection protocols dhcpv4 release]
user@host# set priority medium
```

6. (Optional) Configure how much time must pass since the last violation before the traffic flow is considered to have recovered from the attack.

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

For example, to specify that 600 seconds must have passed since the last violation of the DHCPv4 release packet policer:

```
[edit system ddos-protection protocols dhcpv4 release]
user@host# set recover-time 600
```

7. (Optional) Bypass the aggregate policer configuration. This is relevant only when an aggregate policer is configured for the protocol group.

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

For example, to bypass the aggregate policer for DHCPv4 renew packets:

```
[edit system ddos-protection protocols dhcpv4 renew]
user@host# set bypass-aggregate
```

8. (Optional) Disable line card policers for the packet type on all line cards.

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



NOTE: When you disable line card policers globally at the [edit system ddos-protection global] hierarchy level, the global setting overrides the per-packet type setting shown in this step. If you subsequently remove the global configuration, then the per-packet type configuration takes effect.

For example, to disable the line card policer for DHCPv4 bootp packets:

```
[edit system ddos-protection protocols dhcpv4 bootp]
user@host# set disable-fpc
```

9. (Optional) Disable DDoS event logging for only this packet type.

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



NOTE: Events disabled for the packet are associated with policer violations; logging of flow detection culprit flow events is not affected by this statement.



NOTE: When you disable DDoS event logging globally at the [edit system ddos-protection global] hierarchy level, the global setting overrides the per-packet type setting shown in this step. If you subsequently remove the global configuration, then the per-packet type configuration takes effect.

For example, to disable DDoS event logging line card policer for DHCPv4 discover packets:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set disable-logging
```

10. (Optional) Disable the Routing Engine policer for only this packet type.

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



NOTE: When you disable the Routing Engine policer globally at the [edit system ddos-protection global] hierarchy level, the global setting overrides the per-packet type setting shown in this step. If you subsequently remove the global configuration, then the per-packet type configuration takes effect.

For example, to disable the Routing Engine policer for DHCPv4 discover packets:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set disable-routing-engine
```

11. (Optional) Configure packet-level settings for the packet type on a single line card.

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

For example, to access DHCPv4 discover packet settings on the line card in slot 3:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit fpc 3
```

12. (Optional) Scale the policer bandwidth for the packet type on the line card.

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

For example, to scale the bandwidth to 80 percent of the all-line-card setting configured for DHCPv4 discover packets on the line card in slot 3:

```
[edit system ddos-protection protocols dhcpv4 discover fpc 3]
user@host# edit bandwidth-scale 80
```

13. (Optional) Scale the policer burst size for the packet type on the line card.

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

For example, to scale the maximum bandwidth to 75 percent of the all-line-card setting configured for DHCPv4 discover packets on the line card in slot 3:

```
[edit system ddos-protection protocols dhcpv4 discover fpc 3]
user@host# edit burst-scale 75
```

14. (Optional) Disable the line card policer for the packet type on a particular line card.

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

For example, to disable the line card policer for DHCPv4 discover packets on the line card in slot 3:

```
[edit system ddos-protection protocols dhcpv4 discover fpc 3]
user@host# edit disable-fpc
```

Related Documentation

- [Configuring Protection Against DDoS Attacks on page 15](#)

- For a list of supported protocol groups and packet types, see [protocols on page 65](#).
- [Example: Configuring DDoS Protection on page 23](#)

Disabling DDoS Protection Policers and Logging Globally

DDoS policers are enabled by default for all supported protocol groups and packet types. Policers are established at the level of the individual line card and the Routing Engine. You can disable the line card policers globally for all MPCs or FPC5s. You can also disable the Routing Engine policer. When you disable either of these policers, the policers at that level for all protocol groups and packet types are disabled.

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.



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.

```
[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 15](#)

CHAPTER 5

Example

- [Example: Configuring DDoS Protection on page 23](#)

Example: Configuring DDoS Protection

This example shows how to configure DDoS protection that enables the router to quickly identify an attack and prevent a flood of malicious control packets from exhausting system resources.

- [Requirements on page 23](#)
- [Overview on page 23](#)
- [Configuration on page 24](#)
- [Verification on page 26](#)

Requirements

DDoS protection requires the following hardware and software:

- MX Series 3D Universal Edge Routers that have only MPCs installed or T4000 Core Routers that have only FPC5s installed.



NOTE: If the router has other cards in addition to MPCs or FPC5s, the CLI accepts the configuration but the other cards are not protected and therefore the router is not protected.

- Junos OS Release 11.2 or later

No special configuration beyond device initialization is required before you can configure this feature.

Overview

Distributed denial-of-service attacks use multiple sources to flood a network or router with protocol control packets. This malicious traffic triggers a large number of exceptions in the network and attempts exhaust the system resources to deny valid users access to the network or server.

This example describes how to configure rate-limiting policers that identify excess control traffic and drop the packets before the router is adversely affected. Sample tasks include configuring policers for particular control packet types within a protocol group, configuring an aggregate policer for a protocol group and bypassing that policer for a particular control packet type, 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 in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
[edit]
edit system
set ddos-protection protocols dhcpv4 aggregate bandwidth 669
set ddos-protection protocols dhcpv4 aggregate burst 6000
set ddos-protection protocols dhcpv4 discover bandwidth 100
set ddos-protection protocols dhcpv4 discover recover-time 200
set ddos-protection protocols dhcpv4 discover burst 300
set ddos-protection protocols dhcpv4 offer priority medium
set ddos-protection protocols dhcpv4 offer bypass-aggregate
set ddos-protection protocols dhcpv4 offer fpc 1 bandwidth-scale 80
set ddos-protection protocols dhcpv4 offer fpc 1 burst-scale 75
set ddos-protection protocols pppoe aggregate bandwidth 800
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 dhcpv4
```
2. Configure the maximum traffic rate for the DHCPv4 aggregate policer; that is, for the combination of all DHCPv4 packets.

```
[edit system ddos-protection protocols dhcpv4]
user@host# set aggregate bandwidth 669
```
3. Configure the maximum burst rate for the DHCPv4 aggregate policer.

```
[edit system ddos-protection protocols dhcpv4]
user@host# set aggregate burst 6000
```
4. Configure the maximum traffic rate for the DHCPv4 policer for discover packets.

```
[edit system ddos-protection protocols dhcpv4]
user@host# set discover bandwidth 100
```
5. Decrease the recover time for violations of the DHCPv4 discover policer.

- ```
[edit system ddos-protection protocols dhcpv4]
user@host# set discover recover-time 200
```
6. Configure the maximum burst rate for the DHCPv4 discover policer.
 

```
[edit system ddos-protection protocols dhcpv4]
user@host# set discover burst 300
```
  7. Increase the priority for DHCPv4 offer packets.
 

```
[edit system ddos-protection protocols dhcpv4]
user@host# set offer priority medium
```
  8. Prevent offer packets from being included in the aggregate bandwidth; that is, offer packets do not contribute towards the combined DHCPv4 traffic to determine whether the aggregate bandwidth is exceeded. However, the offer packets are still included in traffic rate statistics.
 

```
[edit system ddos-protection protocols dhcpv4]
user@host# set offer bypass-aggregate
```
  9. Reduce the bandwidth and burst size allowed before violation is declared for the DHCPv4 offer policer on the MPC or FPC5 in slot 1.
 

```
[edit system ddos-protection protocols dhcpv4]
user@host# set offer fpc 1 bandwidth-scale 80
user@host# set offer fpc 1 burst-scale 75
```
  10. Configure the maximum traffic rate for the PPPoE aggregate policer, that is, for the combination of all PPPoE packets.
 

```
[edit system ddos-protection protocols dhcpv4]
user@host# up
[edit system ddos-protection protocols]
user@host# set pppoe aggregate bandwidth 800
```
  11. 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. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit system]
user@host# show ddos-protection
traceoptions {
 file ddos-trace size 10m;
 flag all;
}
protocols {
 pppoe {
 aggregate {
 bandwidth 800;
 }
 }
}
```

```
dhcpv4 {
 aggregate {
 bandwidth 669;
 burst 6000;
 }
 discover {
 bandwidth 100;
 burst 300;
 recover-time 200;
 }
 offer {
 priority medium;
 fpc 1 {
 bandwidth-scale 80;
 burst-scale 75;
 }
 bypass-aggregate;
 }
}
```

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 DHCPv4 DDoS Protection Configuration and Operation on page 26](#)
- [Verifying the PPPoE DDoS Configuration on page 29](#)

---

### Verifying the DHCPv4 DDoS Protection Configuration and Operation

**Purpose** Verify that the DHCPv4 aggregate and protocol policer values have changed from the default. With DHCPv4 and PPPoE traffic flowing, verify that the policers are working correctly. You can enter commands to display the individual policers you are interested in, as shown here, or you can enter the **show ddos-protection protocols dhcpv4** command to display this information for all DHCPv4 packet types.

**Action** From operational mode, enter the **show ddos-protection protocols dhcpv4 aggregate** command.

```
user@host> show ddos-protection protocols dhcpv4 aggregate
Protocol Group: DHCPv4
```

```
Packet type: aggregate (aggregate for all DHCPv4 traffic)
Aggregate policer configuration:
 Bandwidth: 669 pps
 Burst: 6000 packets
 Priority: medium
 Recover time: 300 seconds
 Enabled: Yes
System-wide information:
 Aggregate bandwidth is no longer being violated
 No. of FPCs currently receiving excess traffic: 0
```

```

 No. of FPCs that have received excess traffic: 1
 Violation first detected at: 2011-03-10 06:27:47 PST
 Violation last seen at: 2011-03-10 06:28:57 PST
 Duration of violation: 00:01:10 Number of violations: 1
 Received: 71064 Arrival rate: 0 pps
 Dropped: 23115 Max arrival rate: 1000 pps
Routing Engine information:
 Bandwidth: 669 pps, Burst: 6000 packets, enabled
 Aggregate policer is never violated
 Received: 36130 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 671 pps
 Dropped by aggregate policer: 0
FPC slot 1 information:
 Bandwidth: 100% (669 pps), Burst: 100% (5000 packets), enabled
 Aggregate policer is no longer being violated
 Violation first detected at: 2011-03-10 06:27:48 PST
 Violation last seen at: 2011-03-10 06:28:58 PST
 Duration of violation: 00:01:10 Number of violations: 1
 Received: 71064 Arrival rate: 0 pps
 Dropped: 34934 Max arrival rate: 1000 pps
 Dropped by individual policers: 11819
 Dropped by aggregate policer: 23115

```

From operational mode, enter the **show ddos-protection protocols dhcpv4 discover** command.

```

user@host> show ddos-protection protocols dhcpv4 discover
Protocol Group: DHCPv4

```

```

Packet type: discover (DHCPv4 DHCPDISCOVER)
Individual policer configuration:
 Bandwidth: 100 pps
 Burst: 300 packets
 Priority: low
 Recover time: 200 seconds
 Enabled: Yes
 Bypass aggregate: No
System-wide information:
 Bandwidth is no longer being violated
 No. of FPCs currently receiving excess traffic: 0
 No. of FPCs that have received excess traffic: 1
 Violation first detected at: 2011-03-10 06:28:34 PST
 Violation last seen at: 2011-03-10 06:28:55 PST
 Duration of violation: 00:00:21 Number of violations: 1
 Received: 47949 Arrival rate: 0 pps
 Dropped: 11819 Max arrival rate: 671 pps
Routing Engine information:
 Bandwidth: 100 pps, Burst: 300 packets, enabled
 Policer is never violated
 Received: 36130 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
 Dropped by aggregate policer: 0
FPC slot 1 information:
 Bandwidth: 100% (100 pps), Burst: 100% (300 packets), enabled
 Policer is no longer being violated
 Violation first detected at: 2011-03-10 06:28:35 PST
 Violation last seen at: 2011-03-10 06:28:55 PST
 Duration of violation: 00:00:20 Number of violations: 1
 Received: 47949 Arrival rate: 0 pps
 Dropped: 11819 Max arrival rate: 671 pps

```

```
Dropped by this policer: 11819
Dropped by aggregate policer: 0
```

From operational mode, enter the **show ddos-protection protocols dhcpv4 offer** command.

```
user@host> show ddos-protection protocols dhcpv4 offer
Protocol Group: DHCPv4
```

```
Packet type: offer (DHCPv4 DHCP OFFER)
Individual policer configuration:
 Bandwidth: 1000 pps
 Burst: 1000 packets
 Priority: medium
 Recover time: 300 seconds
 Enabled: Yes
 Bypass aggregate: Yes
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:
 Bandwidth: 80% (800 pps), Burst: 75% (750 packets), enabled
 Policer is never violated
 Received: 0 Arrival rate: 0 pps
 Dropped: 0 Max arrival rate: 0 pps
 Dropped by aggregate policer: 0
```

**Meaning** The output of these commands lists the policer configuration and traffic statistics for the DHCPv4 aggregate, discover, and offer policers respectively.

The **Aggregate policer configuration** section in the first output example and **Individual policer configuration** sections in the second and third output examples list the configured values for bandwidth, burst, priority, recover time, and bypass-aggregate.

The **System-wide information** section shows the total of all DHCPv4 traffic statistics and violations for the policer recorded across all line cards and at the Routing Engine. The **Routing engine information** section shows the traffic statistics and violations for the policer recorded at the Routing Engine. The **FPC slot 1 information** section shows the traffic statistics and violations for the policer recorded only at the line card in slot 1.

The output for the aggregate policer in this example shows the following information:

- The **System-wide information** section shows that 71,064 DHCPv4 packets of all types were received across all line cards and the Routing Engine. The section shows a single violation with a time stamp and that the aggregate policer at a line card dropped 23,115 of these packets.
- The **FPC slot 1 information** section shows that this line card received all 71,064 DHCPv4 packets, but its aggregate policer experienced a violation and dropped the 23,115 packets shown in the other section. The line card individual policers dropped an additional 11,819 packets.

- The **Routing Engine information** section shows that the remaining 36,130 packets all reached the Routing Engine and that its aggregate policer dropped no additional packets.

The difference between the number of DHCPv4 packets received and dropped at the line card  $[71,064 - (23,115 + 11,819)]$  matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 1 received any DHCPv4 packets.

The output for the DHCPv4 discover packet policer in this example shows the following information:

- The **System-wide information** section shows that 47,949 DHCPv4 discover packets were received across all line cards and the Routing Engine. The section shows a single violation with a time stamp and that the aggregate policer at a line card dropped 11,819 of these packets.
- The **FPC slot 1 information** section shows that this line card received all 47,949 DHCPv4 discover packets, but its individual policer experienced a violation and dropped the 11,819 packets shown in the other section.
- The **Routing Engine information** section shows that only 36,130 DHCPv4 discover packets reached the Routing Engine and that it dropped no additional packets.

The difference between the number of DHCPv4 discover packets received and dropped at the line card  $(47,949 - 11,819)$  matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 1 received any DHCPv4 discover packets.

The output for the DHCPv4 offer packet policer in this example shows the following information:

- This individual policer has never been violated at any location.
- No DHCPv4 offer packets have been received at any location.

### Verifying the PPPoE DDoS Configuration

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

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

```
user@host> show ddos-protection protocols pppoe parameters brief
Number of policers modified: 1
Protocol Packet Bandwidth Burst Priority Recover Policer Bypass FPC
group type (pps) (pkts) time(sec) enabled aggr. mod
pppoe aggregate 800* 2000 medium 300 yes -- no
pppoe padi 500 500 low 300 yes no no
pppoe pado 0 0 low 300 yes no no
pppoe padr 500 500 medium 300 yes no no
pppoe pads 0 0 low 300 yes no no
pppoe padt 1000 1000 high 300 yes no no
```

|       |      |   |   |     |     |     |    |    |
|-------|------|---|---|-----|-----|-----|----|----|
| pppoe | padm | 0 | 0 | low | 300 | yes | no | no |
| pppoe | padn | 0 | 0 | low | 300 | yes | no | no |

From operational mode, enter the **show ddos-protection protocols pppoe padi** command, and enter the command for **padr** as well.

```
user@host> show ddos-protection protocols pppoe padi
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
System-wide information:
 Bandwidth for this packet type is being violated!
 Number of slots currently receiving excess traffic: 1
 Number of slots that have received excess traffic: 1
 Violation first detected at: 2011-03-09 11:26:33 PST
 Violation last seen at: 2011-03-10 12:03:44 PST
 Duration of violation: 1d 00:37 Number of violations: 1
 Received: 704832908 Arrival rate: 8000 pps
 Dropped: 660788548 Max arrival rate: 8008 pps
Routing Engine information:
 Bandwidth: 500 pps, Burst: 500 packets, enabled
 Policer is never violated
 Received: 39950330 Arrival rate: 298 pps
 Dropped: 0 Max arrival rate: 503 pps
 Dropped by aggregate policer: 0
FPC slot 3 information:
 Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
 Policer is currently being violated!
 Violation first detected at: 2011-03-09 11:26:35 PST
 Violation last seen at: 2011-03-10 12:03:44 PST
 Duration of violation: 1d 00:37 Number of violations: 1
 Received: 704832908 Arrival rate: 8000 pps
 Dropped: 664882578 Max arrival rate: 8008 pps
 Dropped by this policer: 660788548
 Dropped by aggregate policer: 4094030
```

```
user@host> show ddos-protection protocols pppoe padr
Protocol Group: PPPoE
```

```
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
System-wide information:
 Bandwidth for this packet type is being violated!
 Number of slots currently receiving excess traffic: 1
 Number of slots that have received excess traffic: 1
 Violation first detected at: 2011-03-10 06:21:17 PST
 Violation last seen at: 2011-03-10 12:04:14 PST
 Duration of violation: 05:42:57 Number of violations: 1
```

```

Received: 494663595 Arrival rate: 24038 pps
Dropped: 484375900 Max arrival rate: 24062 pps
Routing Engine information:
Bandwidth: 500 pps, Burst: 500 packets, enabled
Policer is never violated
Received: 10287695 Arrival rate: 500 pps
Dropped: 0 Max arrival rate: 502 pps
Dropped by aggregate policer: 0
FPC slot 1 information:
Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
Policer is currently being violated!
Violation first detected at: 2011-03-10 06:21:18 PST
Violation last seen at: 2011-03-10 12:04:14 PST
Duration of violation: 05:42:56 Number of violations: 1
Received: 494663595 Arrival rate: 24038 pps
Dropped: 484375900 Max arrival rate: 24062 pps
Dropped by this policer: 484375900
Dropped by aggregate policer: 0

```

**Meaning** The output from the **show ddos-protection protocols pppoe parameters brief** command lists the current configuration for each of the individual PPPoE packet policers and the PPPoE aggregate policer. A change from a default value is indicated by an asterisk next to the modified value. The only change made to PPPoE policers in the configuration steps was to the aggregate policer bandwidth; this change is confirmed in the output. Besides the configuration values, the command output also reports whether a policer has been disabled, whether it bypasses the aggregate policer (meaning that the traffic for that packet type is not included for evaluation by the aggregate policer), and whether the policer has been modified for one or more line cards.

The output of the **show ddos-protection protocols pppoe padi** command in this example shows the following information:

- The **System-wide information** section shows that 704,832,908 PPPoE PADI packets were received across all line cards and the Routing Engine. The section shows a single violation on a line card that is still in progress, and that the aggregate policer at the line card dropped 660,788,548 of the PADI packets.
- The **FPC slot 3 information** section shows that this line card received all 704,832,908 PADI packets. Its individual policer dropped 660,788,548 of those packets and its aggregate policer dropped the other 4,094,030 packets. The violation is ongoing and has lasted more than a day.
- The **Routing Engine information** section shows that only 39,950,330 PADI packets reached the Routing Engine and that it dropped no additional packets.

The difference between the number of PADI packets received and dropped at the line card  $[704,832,908 - (660,788,548 + 4,094,030)]$  matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 3 received any PADI packets.

The output of the **show ddos-protection protocols pppoe padr** command in this example shows the following information:

- The **System-wide information** section shows that 494,663,595 PPPoE PADR packets were received across all line cards and the Routing Engine. The section shows a single violation on a line card that is still in progress, and that the policer at the line card dropped 484,375,900 of the PADR packets.
- The **FPC slot 1 information** section shows that this line card received all 494,663,595 PADR packets. Its individual policer dropped 484,375,900 of those packets. The violation is ongoing and has lasted more than five hours.
- The **Routing Engine information** section shows that only 10,287,695 PADR packets reached the Routing Engine and that it dropped no additional packets.

The difference between the number of PADR packets received and dropped at the line card (494,663,595 - 484,375,900) matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 1 received any PADR packets.



**NOTE:** This scenario is unrealistic in showing all PADI packets received on one line card and all PADR packets on a different line card. The intent of the scenario is to illustrate how policer violations are reported for individual line cards.

**Related  
Documentation**

- [Distributed Denial-of-Service \(DDoS\) Protection Overview on page 3](#)
- [Configuring Protection Against DDoS Attacks on page 15](#)



# Configuration Overview for Flow Detection

- [Configuring Flow Detection for DDoS Protection on page 33](#)

## Configuring Flow Detection for DDoS Protection

---

Flow detection monitors the flows of control traffic for violation of the bandwidth allowed for each flow and manages traffic identified as a culprit flow. Suppression of the traffic is the default management option. Flow detection is typically implemented as part of an overall DDoS protection strategy, but it is also useful for troubleshooting and understanding traffic flow in new configurations. Flow detection is disabled by default.

Before you begin, ensure you have configured DDoS protection appropriately for your network. See [“Configuring Protection Against DDoS Attacks” on page 15](#) for detailed information about DDoS protection.

To configure flow detection:

1. Enable flow detection globally for all protocol groups and packet types.  
[See “Enabling Flow Detection for All Protocol Groups and Packet Types” on page 37.](#)
2. (Optional) Set the rate at which culprit flow events are reported for all line cards, protocol groups, and packet types.  
[See “Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types” on page 37.](#)
3. Set the rate at which bandwidth violations are reported for all line cards, protocol groups, and packet types.  
[See “Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types” on page 37.](#)
4. (Optional) Configure how long a suspicious flow must be in violation of flow bandwidth before being declared a culprit flow.  
[See “Configuring the Detection Period for Suspicious Flows” on page 38.](#)
5. (Optional) Configure how long a culprit flow must drop to within its allowed bandwidth before being declared normal.  
[See “Configuring the Recovery Period for a Culprit Flow” on page 38.](#)
6. (Optional) Enable and configure how long a culprit flow is suppressed or monitored.

See [“Configuring the Timeout Period for a Culprit Flow”](#) on page 39.

7. (Optional) Configure when flow detection monitors flows.

See [“Configuring Flow Detection for Individual Protocol Groups or Packets”](#) on page 40.

8. (Optional) Configure when flow detection operates at each flow aggregation level (subscriber, logical interface, and physical interface).

See [“Configuring How Flow Detection Operates at Each Flow Aggregation Level”](#) on page 40.

9. Configure the maximum bandwidth for packet flows at each flow aggregation level (subscriber, logical interface, and physical interface).

See [“Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level”](#) on page 42.

10. (Optional) Configure how traffic is controlled at each flow aggregation level (subscriber, logical interface, and physical interface) for flows that violate their bandwidth.

See [“Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level”](#) on page 42.

11. (Optional) Disable automatic logging of suspicious flows.

See [“Disabling Automatic Logging of Culprit Flow Events for a Packet Type”](#) on page 43.

**Related  
Documentation**

- [Distributed Denial-of-Service \(DDoS\) Protection Overview](#) on page 3
- [DDoS Protection Flow Detection Overview](#) on page 9

## CHAPTER 7

# Configuration Tasks for Flow Detection

- [Configuring Flow Detection for DDoS Protection on page 35](#)
- [Enabling Flow Detection for All Protocol Groups and Packet Types on page 37](#)
- [Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types on page 37](#)
- [Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types on page 37](#)
- [Configuring the Detection Period for Suspicious Flows on page 38](#)
- [Configuring the Recovery Period for a Culprit Flow on page 38](#)
- [Configuring the Timeout Period for a Culprit Flow on page 39](#)
- [Configuring Flow Detection for Individual Protocol Groups or Packets on page 40](#)
- [Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 40](#)
- [Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 42](#)
- [Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 42](#)
- [Disabling Automatic Logging of Culprit Flow Events for a Packet Type on page 43](#)

### Configuring Flow Detection for DDoS Protection

Flow detection monitors the flows of control traffic for violation of the bandwidth allowed for each flow and manages traffic identified as a culprit flow. Suppression of the traffic is the default management option. Flow detection is typically implemented as part of an overall DDoS protection strategy, but it is also useful for troubleshooting and understanding traffic flow in new configurations. Flow detection is disabled by default.

Before you begin, ensure you have configured DDoS protection appropriately for your network. See [“Configuring Protection Against DDoS Attacks” on page 15](#) for detailed information about DDoS protection.

To configure flow detection:

1. Enable flow detection globally for all protocol groups and packet types.  
See [“Enabling Flow Detection for All Protocol Groups and Packet Types” on page 37.](#)
2. (Optional) Set the rate at which culprit flow events are reported for all line cards, protocol groups, and packet types.  
See [“Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types” on page 37.](#)
3. Set the rate at which bandwidth violations are reported for all line cards, protocol groups, and packet types.  
See [“Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types” on page 37.](#)
4. (Optional) Configure how long a suspicious flow must be in violation of flow bandwidth before being declared a culprit flow.  
See [“Configuring the Detection Period for Suspicious Flows” on page 38.](#)
5. (Optional) Configure how long a culprit flow must drop to within its allowed bandwidth before being declared normal.  
See [“Configuring the Recovery Period for a Culprit Flow” on page 38.](#)
6. (Optional) Enable and configure how long a culprit flow is suppressed or monitored.  
See [“Configuring the Timeout Period for a Culprit Flow” on page 39.](#)
7. (Optional) Configure when flow detection monitors flows.  
See [“Configuring Flow Detection for Individual Protocol Groups or Packets” on page 40.](#)
8. (Optional) Configure when flow detection operates at each flow aggregation level (subscriber, logical interface, and physical interface).  
See [“Configuring How Flow Detection Operates at Each Flow Aggregation Level” on page 40.](#)
9. Configure the maximum bandwidth for packet flows at each flow aggregation level (subscriber, logical interface, and physical interface).  
See [“Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level” on page 42.](#)
10. (Optional) Configure how traffic is controlled at each flow aggregation level (subscriber, logical interface, and physical interface) for flows that violate their bandwidth.  
See [“Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level” on page 42.](#)
11. (Optional) Disable automatic logging of suspicious flows.  
See [“Disabling Automatic Logging of Culprit Flow Events for a Packet Type” on page 43.](#)

- Related Documentation**
- [Distributed Denial-of-Service \(DDoS\) Protection Overview on page 3](#)
  - [DDoS Protection Flow Detection Overview on page 9](#)

## Enabling Flow Detection for All Protocol Groups and Packet Types

---

By default, flow detection is disabled for all protocol groups and packet types. You must enable flow detection globally by including the **flow-detection** statement. If you subsequently disable flow detection for individual packet types, you cannot use this global statement to override all such individual configurations; you must re-enable detection at the packet configuration level.

To enable flow detection globally:

- Set flow detection.

```
[edit system ddos-protection global]
user@host# set flow-detection
```

- Related Documentation**
- [Configuring Flow Detection for DDoS Protection on page 33](#)
  - [Configuring Protection Against DDoS Attacks on page 15](#)

## Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types

---

When flow detection confirms that a suspicious flow it is tracking on a line card is indeed a culprit flow, it sends a report to the Routing Engine. Flow detection also reports each culprit flow that subsequently recovers to within the allowed bandwidth or is cleared. You can include the **flow-report-rate** statement to limit how many flows per second on each line card can be reported. Culprit flow events are reported for all protocol groups and packet types by default. When too many flows are reported, congestion can occur on the host path to the Routing Engine flow.

To globally configure the maximum report rate for culprit flows:

- Set the reporting rate.

```
[edit system ddos-protection global]
user@host# set flow-report-rate rate
```

- Related Documentation**
- [Configuring Flow Detection for DDoS Protection on page 33](#)
  - [Disabling Automatic Logging of Culprit Flow Events for a Packet Type on page 43](#)

## Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types

---

By default, flow detection reports to the Routing Engine all violations of bandwidth at the FPC for all protocol groups and packet types. You can include the **violation-report-rate** statement to limit how many violations per second flow detection reports from the line

cards, thus reducing the load on the router. We recommend that you configure a report rate that is suitable for your network rather than rely on the default value.

To globally configure the maximum bandwidth violation reporting rate:

- Set the reporting rate.

```
[edit system ddos-protection global]
user@host# set violation-report-rate rate
```

Related  
Documentation

- [Configuring Flow Detection for DDoS Protection on page 33](#)

---

## Configuring the Detection Period for Suspicious Flows

DDoS protection flow detection considers a monitored flow to be a suspicious flow whenever the flow exceeds its allowed bandwidth, based on a crude test that eliminates obviously good flows from consideration. A closer examination of a suspicious flow requires the flow to remain in violation of the bandwidth for a period of time before flow detection considers it to be a culprit flow against which it must take action. You can include the **flow-detect-time** statement to configure the duration of this detection period or you can rely on the default period of three seconds.



**BEST PRACTICE:** We recommend that you use the default value for the detection period.

To specify how long a flow must be in violation before flow detection declares it to be a culprit flow:

- Set the detection period.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set flow-detect-time seconds
```

For example, include the following statement to require the DHCPv4 discover packet flow to be in violation of its allowed bandwidth for 30 seconds before it is considered to be a culprit flow:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set flow-detect-time 30
```

Related  
Documentation

- [Configuring Flow Detection for DDoS Protection on page 33](#)

---

## Configuring the Recovery Period for a Culprit Flow

After DDoS protection flow detection has identified a suspicious flow as a culprit flow, it has to determine when that flow no longer represents a threat to the router. When the traffic flow rate drops back to within the allowed bandwidth, the rate must remain within the bandwidth for a recovery period. Only then does flow detection consider the flow to be normal and stop the traffic handling action enacted against the culprit flow. You can

include the **flow-recover-time** statement to configure the duration of this recovery period or you can rely on the default period of 60 seconds.

To specify how long a flow must be within its allowed bandwidth after a violation before flow detection declares it to be a normal flow:

- Set the recovery period.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set flow-recover-time seconds
```

For example, include the following statement to require the DHCPv4 discover packet flow to be in recovery for five minutes (300 seconds):

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set flow-recover-time 300
```

#### Related Documentation

- [Configuring Flow Detection for DDoS Protection on page 33](#)

## Configuring the Timeout Period for a Culprit Flow

When DDoS protection flow detection identifies a suspicious flow as a culprit flow, by default it suppresses traffic for that flow for as long as the traffic flow exceeds the bandwidth limit. Suppression stops and the flow is removed from the flow table when the time since the last violation by the flow is greater than the recovery period.

Alternatively, you can include the **timeout-active-flows** statement to enable flow detection to suppress a culprit flow for a configurable timeout period. When the timeout period expires, suppression stops and the flow is removed from the flow table. You can either include the **flow-timeout-time** statement to configure the duration of the timeout period or rely on the default timeout of 300 seconds.

To enable flow detection to suppress a culprit flow for a timeout period:

1. Enable the timeout.

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

2. Specify the timeout period.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set flow-timeout-time seconds
```

For example, include the following statements to suppress the DHCPv4 discover packet flow for 10 minutes (600 seconds):

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set timeout-active-flows
user@host# set flow-timeout-time 600
```

#### Related Documentation

- [Configuring Flow Detection for DDoS Protection on page 33](#)

## Configuring Flow Detection for Individual Protocol Groups or Packets

---

By default, flow detection is disabled for all protocol groups and packet types. After you have turned on flow detection globally, you can include the **flow-detection-mode** statement to configure flow detection to operate differently for individual packet types. By default, flow detection operates in automatic mode for all packet types, meaning that it monitors control traffic for suspicious flows only after a DDoS policer has been violated. You can also configure flow detection either to never monitor flows or to always monitor flows.



**NOTE:** The flow detection mode at the packet level must be either **automatic** or **on** for flow detection to operate at individual flow aggregation levels.

To configure how flow detection operates:

- Disable suspicious flow detection for a packet type.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set flow-detection-mode off
```

- Set flow detection to operate automatically when a policer is violated.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set flow-detection-mode automatic
```

- Specify that flow detection is always on for a packet type.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set flow-detection-mode on
```

### Related Documentation

- [Configuring Flow Detection for DDoS Protection on page 33](#)
- [Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 40](#)

## Configuring How Flow Detection Operates at Each Flow Aggregation Level

---

When flow detection is turned on, traffic flows are monitored by default for all protocol groups and packet types. When a policer violation occurs, each suspicious flow is examined to determine whether it is the culprit flow that caused the violation. You can include the **flow-level-detection** statement to configure how flow detection works at each flow aggregation level for a packet type: subscriber, logical interface, or physical interface.



**NOTE:** The flow detection mode at the packet level must be either **automatic** or **on** for flow detection to operate at individual flow aggregation levels.



Flow detection supports three operation modes:

- **automatic**—When a DDoS protection policer is violated, traffic flows at this flow aggregation level are monitored for suspicious behavior only until flow detection determines that the suspect flow is not at this aggregation level and instead must be at a coarser level of aggregation. Flows at this level are subsequently not searched again until the policer is no longer violated at the coarser level.
- **off**—Traffic flows are never monitored at this flow aggregation level.
- **on**—Traffic flows at this flow aggregation level are monitored for suspicious flows even when no DDoS protection policer is currently being violated, if flow detection at the packet level is configured to **on**. Monitoring continues at this level regardless of whether a suspect flow is identified at this level. However, if the packet level mode is **automatic**, then the policer must be in violation for traffic flows to be checked at this level.

Flows are examined first at the finest-grained (lowest bandwidth) flow aggregation level, subscriber. If the suspect flow is not found at the subscriber level, then flows are checked at the logical interface level. Finally, if the suspect is not found there, then flows are checked at the physical interface level; barring some misconfiguration, the culprit flow must be found at this level.

To configure how flow detection operates at each flow aggregation level:

1. (Optional) Specify the detection mode at the subscriber level.

```
[edit system ddos-protection protocols protocol-group packet-type flow-level-detection]
user@host# set subscriber flow-operation-mode
```

2. (Optional) Specify the detection mode at the logical interface level.

```
[edit system ddos-protection protocols protocol-group packet-type flow-level-detection]
user@host# set logical-interface flow-operation-mode
```

3. (Optional) Specify the detection mode at the physical interface level.

```
[edit system ddos-protection protocols protocol-group packet-type flow-level-detection]
user@host# set physical-interface flow-operation-mode
```

For example, include the following statements to configure flow detection to check for suspicious flows at the subscriber level only when the policer is being violated, to never check at the logical interface level, and to always check at the physical interface level:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit flow-level-detection
user@host# set subscriber automatic
user@host# set logical-interface off
user@host# set physical-interface on
```

#### Related Documentation

- [Configuring Flow Detection for DDoS Protection on page 33](#)
- [Configuring Flow Detection for Individual Protocol Groups or Packets on page 40](#)

## Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level

You can include the **flow-level-bandwidth** statement to configure the maximum acceptable bandwidth for traffic flows for individual packet types. You have to specify the bandwidth behavior at a particular flow aggregation level: subscriber, logical interface, or physical interface. We recommend that you tune the bandwidth values for your network rather than rely on the defaults.

To configure the maximum bandwidth for traffic flows each flow aggregation level:

1. (Optional) Configure the bandwidth for flows at the subscriber level.

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

2. (Optional) Configure the bandwidth for flows at the logical interface level.

```
[edit system ddos-protection protocols protocol-group packet-type
 flow-level-bandwidth]
user@host# set logical-interface flow-bandwidth
```

3. (Optional) Configure the bandwidth for flows at the physical interface level.

```
[edit system ddos-protection protocols protocol-group packet-type
 flow-level-bandwidth]
user@host# set physical-interface flow-bandwidth
```

For example, to configure the flow bandwidth to 1000 pps at the subscriber level, 5000 pps at the logical interface level, and 30,000 at the physical interface level:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit flow-level-bandwidth
user@host# set subscriber 10
user@host# set logical-interface 100
user@host# set physical-interface 1000
```

### Related Documentation

- [Configuring Flow Detection for DDoS Protection on page 33](#)

## Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level

When flow detection is enabled, all traffic in a culprit flow is dropped by default for all protocol groups and packet types and at all flow aggregation levels. You can include the **flow-level-control** statement to configure flow detection to control traffic differently for individual packet types. You have to specify the control behavior at a particular flow aggregation level: subscriber, logical interface, or physical interface.

You can configure flow detection flow control to employ one of the following modes for a packet type:

- Drop all traffic—Configure flow control to drop all traffic when you think the flow that is violating a bandwidth limit is malicious. This behavior is the default at all flow aggregation levels.

- **Police traffic**—Configure flow control to police a flow that is violating bandwidth, forcing the rate below the bandwidth limit. Flow control acts as a simple policer in this case.
- **Keep all traffic**—Configure flow control to keep all traffic whether the flow is in violation or below the bandwidth limit. This mode is helpful when you need to debug traffic flow for your network.

Flow control mode enables great flexibility in how you manage control traffic in your network. For example, if you only want to ensure that control flows for a packet type at all aggregation levels are within their limits, you can configure flow control to police the traffic at each level. Or if you want to detect culprit flows and suppress them at one level but only restrain traffic to the allowed bandwidth at another level, you can configure one level to drop all traffic and the other to police traffic.

To configure how flow detection controls traffic in a culprit flow:

1. (Optional) Specify the control mode at the subscriber level.

```
[edit system ddos-protection protocols protocol-group packet-type scfd
flow-level-control]
user@host# set subscriber flow-control-mode
```

2. (Optional) Specify the control mode at the logical interface level.

```
[edit system ddos-protection protocols protocol-group packet-type scfd
flow-level-control]
user@host# set logical-interface flow-control-mode
```

3. (Optional) Specify the control mode at the physical interface level.

```
[edit system ddos-protection protocols protocol-group packet-type scfd
flow-level-control]
user@host# set physical-interface flow-control-mode
```

For example, to configure flow detection to keep all traffic for a physical interface under the configured bandwidth, but detect and suppress culprit flows at the subscriber level:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit flow-level-control
user@host# set subscriber drop
user@host# set physical-interface police
user@host# edit flow-level-detection
user@host# set logical-interface off
```

In this example, you do not care about the logical interface, so flow detection is turned off for that level. Because flow detection is disabled, the state of flow control for that level does not matter.

#### Related Documentation

- [Configuring Flow Detection for DDoS Protection on page 33](#)

## Disabling Automatic Logging of Culprit Flow Events for a Packet Type

By default, flow detection automatically logs policer violation events associated with suspicious flows (violation reports) and culprit flow events (flow reports) for all protocol groups and packet types. You can include the **no-flow-logging** statement to prevent

automatic logging of culprit flow events for individual packet types. Automatic logging of suspicious flow violation events is disabled with the **disable-logging** statement at the **[edit system ddos-protection global]** hierarchy level.

To disable automatic culprit flow event logging for a packet type:

- Disable logging.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set no-flow-logging
```

To disable automatic suspicious flow violation event logging for a packet type:

- Disable logging.

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

For example, include the following statement to disable automatic logging for DHCPv4 DISCOVER packet flows:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set no-flow-logging
```

**Related  
Documentation**

- [Configuring Flow Detection for DDoS Protection on page 33](#)
- [Configuring DDoS Protection Policers for Individual Packet Types on page 17](#)

## CHAPTER 8

# Configuration Statements

- [\[edit system ddos-protection\] Hierarchy Level on page 45](#)

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

---

```
system {
 ddos-protection {
 global {
 disable-fpc;
 disable-logging;
 disable-routing-engine;
 flow-detection;
 flow-report-rate;
 violation-report-rate;
 }
 protocols protocol-group (aggregate | packet-type) {
 bandwidth packets-per-second;
 burst size;
 bypass-aggregate;
 disable-fpc;
 disable-logging;
 disable-routing-engine;
 flow-detection-mode (automatic | off | on);
 flow-detect-time seconds;
 flow-level-bandwidth {
 logical-interface flow-bandwidth;
 physical-interface flow-bandwidth;
 subscriber flow-bandwidth;
 }
 flow-level-control {
 logical-interface flow-control-mode;
 physical-interface flow-control-mode;
 subscriber flow-control-mode;
 }
 flow-level-detection {
 logical-interface flow-operation-mode;
 physical-interface flow-operation-mode;
 subscriber flow-operation-mode;
 }
 flow-recover-time seconds;
 flow-timeout-time seconds;
 fpc slot-number {
```

```

 bandwidth-scale percentage;
 burst-scale percentage;
 disable-fpc;
 }
 no-flow-logging
 priority level;
 recover-time seconds; timeout-active-flows;
}
re-services {
 captive-portal {
 bandwidth packets-per-second;
 burst size;
 }
}
traceoptions{
 file filename <files number> <match regular-expression > <size maximum-file-size>
 <world-readable | no-world-readable>;
 flag flag;
 level (all | error | info | notice | verbose | warning);
 no-remote-trace;
}
}
}

```

- Related Documentation**
- [Configuring Protection Against DDoS Attacks on page 15](#)
  - [Configuring Flow Detection for DDoS Protection on page 33](#)

## bandwidth (DDoS)

|                                 |                                                                                                                                                                                                                                                   |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>bandwidth <i>packets-per-second</i></code> ;                                                                                                                                                                                                |
| <b>Hierarchy Level</b>          | [edit system ddos-protection <b>protocols</b> <i>protocol-group</i> (aggregate   <i>packet-type</i> )]                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.                                                                                                                                                                                                    |
| <b>Description</b>              | (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Configure the DDoS bandwidth rate limit; the maximum traffic rate (packets per second) allowed for the packet type. When the value is exceeded, a violation is declared. |
| <b>Options</b>                  | <b><i>packets-per-second</i></b> —Number of packets per second that are allowed for the packet type.<br><b>Range:</b> 1 through 100,000 packets per second                                                                                        |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring DDoS Protection Policers for Individual Packet Types on page 17</a></li> </ul>                                                                                                   |

## bandwidth-scale (DDoS)

|                                 |                                                                                                                                                                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>bandwidth-scale <i>percentage</i>;</code>                                                                                                                                                                                 |
| <b>Hierarchy Level</b>          | [edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> ) <b>fpc</b> <i>slot-number</i> ]                                                                                                  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.                                                                                                                                                                                  |
| <b>Description</b>              | (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Configure the percentage by which the DDoS bandwidth rate limit is scaled down for the packet type 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.</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>                                                                                                      |

## burst (DDoS)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>burst <i>size</i>;</code>                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit system ddos-protection <b>protocols</b> <i>protocol-group</i> (aggregate   <i>packet-type</i> )]                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.                                                                                                                                                                                                                                                                                                                                                         |
| <b>Description</b>              | (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Configure the DDoS burst limit; the maximum number of packets of the packet type that is allowed in a burst of traffic. When this value is exceeded, a violation is declared.                                                                                                                                                 |
| <b>Options</b>                  | <p><b><i>size</i></b>—Number of packets that are allowed in a burst for the packet type.</p> <p><b>Range:</b> 1 through 100,000 packets</p> <p><b>Default:</b> The default burst value varies by packet type. You can view the default values for all packet types on an unconfigured router by entering the <b>show ddos-protection protocols parameters brief</b> command from operational mode.</p> |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                             |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring DDoS Protection Policers for Individual Packet Types on page 17</a></li> </ul>                                                                                                                                                                                                                                                        |

## burst-scale (DDoS)

---

|                                 |                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>burst-scale <i>percentage</i>;</code>                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> ) <b>fpc</b> <i>slot-number</i> ]                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.                                                                                                                                                           |
| <b>Description</b>              | (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Configure the percentage by which the DDoS burst limit is scaled down for the packet type on the specified card.                |
| <b>Options</b>                  | <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.<br><b>Range:</b> 1 through 100 percent<br><b>Default:</b> 100 |
| <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 on page 17</a></li></ul>                                                            |

## bypass-aggregate (DDoS)

---

|                                 |                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>bypass-aggregate;</code>                                                                                                                                                                                              |
| <b>Hierarchy Level</b>          | [edit system ddos-protection <b>protocols</b> <i>protocol-group</i> <i>packet-type</i> ]                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.                                                                                                                                                                              |
| <b>Description</b>              | (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) 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 on page 17</a></li></ul>                                                                               |



## ddos-protection (DDoS)

```
Syntax ddos-protection
 global {
 disable-fpc;
 disable-logging;
 disable-routing-engine;
 flow-detection;
 flow-report-rate;
 violation-report-rate;
 }
 protocols protocol-group (aggregate | packet-type) {
 bandwidth packets-per-second;
 burst size;
 bypass-aggregate;
 disable-fpc;
 disable-logging;
 disable-routing-engine;
 flow-detection-mode (automatic | off | on);
 flow-detect-time seconds;
 flow-level-bandwidth {
 logical-interface flow-bandwidth;
 physical-interface flow-bandwidth;
 subscriber flow-bandwidth;
 }
 flow-level-control {
 logical-interface flow-control-mode;
 physical-interface flow-control-mode;
 subscriber flow-control-mode;
 }
 flow-level-detection {
 logical-interface flow-operation-mode;
 physical-interface flow-operation-mode;
 subscriber flow-operation-mode;
 }
 flow-recover-time seconds;
 flow-timeout-time seconds;
 fpc slot-number {
 bandwidth-scale percentage;
 burst-scale percentage;
 disable-fpc;
 }
 no-flow-logging
 priority level;
 recover-time seconds;
 timeout-active-flows;
 }
 re-services {
 captive-portal {
 bandwidth packets-per-second;
 burst size;
 }
 }
 traceoptions{
```

```
file filename <files number> <match regular-expression > <size maximum-file-size>
 <world-readable | no-world-readable>;
flag flag;
level (all | error | info | notice | verbose | warning);
no-remote-trace;
}
}
```

|                          |                                                                                                                                                                                                              |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hierarchy Level          | [edit system]                                                                                                                                                                                                |
| Release Information      | Statement introduced in Junos OS Release 11.2.                                                                                                                                                               |
| Description              | Configure DDoS policers.<br><br>The remaining statements are explained separately.                                                                                                                           |
| Required Privilege Level | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                              |
| Related Documentation    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Protection Against DDoS Attacks on page 15</a></li><li>• <a href="#">Configuring Flow Detection for DDoS Protection on page 33</a></li></ul> |

---

## disable-fpc (DDoS)

---

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | disable-fpc;                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Hierarchy Level          | [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> ]                                                                                                                      |
| Release Information      | 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.                                                                                                                                                                                                         |
| Description              | (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) 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. |
| Required Privilege Level | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                                                                                                                                               |
| Related Documentation    | <ul style="list-style-type: none"><li>• <a href="#">Disabling DDoS Protection Policers and Logging Globally on page 21</a></li><li>• <a href="#">Configuring DDoS Protection Policers for Individual Packet Types on page 17</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.                                                                                                                                    |
| <b>Description</b>              | (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Disable router-wide logging of all DDoS violation and flow detection events globally. Disable only logging of events other than flow detection culprit flow events for a particular packet type within a protocol group. Typically used for debugging purposes.                 |
| <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 21</a></li> <li>• <a href="#">Configuring DDoS Protection Policers for Individual Packet Types on page 17</a></li> <li>• <a href="#">Disabling Automatic Logging of Culprit Flow Events for a Packet Type on page 43</a></li> </ul> |

## disable-routing-engine (DDoS)

|                                 |                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | disable-routing-engine;                                                                                                                                                                                                                                                                                          |
| <b>Hierarchy Level</b>          | [edit system ddos-protection <a href="#">global</a> ],<br>[edit system ddos-protection <a href="#">protocols</a> <i>protocol-group</i> (aggregate   <i>packet-type</i> )]                                                                                                                                        |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Disable DDoS Routing Engine policers for debugging purposes for a particular packet type within a protocol group or globally for all packet types in all protocols. This statement does not affect the state of the line card policers. |
| <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 21</a></li> </ul>                                                                                                                                                                           |

## flow-detection (DDoS Flow Detection)

---

|                                 |                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | flow-detection;                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit system ddos-protection <a href="#">global</a> ]                                                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                    |
| <b>Description</b>              | (MX Series routers with MPCs only) Enable flow detection globally for all protocol groups and packet types.                                                                                                                       |
| <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="#">Enabling Flow Detection for All Protocol Groups and Packet Types on page 37</a></li><li>• <a href="#">Configuring Flow Detection for DDoS Protection on page 33</a></li></ul> |

## flow-detection (DDoS Packet Level)

```
Syntax flow-detection {
 flow-detect-time detect-period;
 no-flow-logging;
 timeout-active-flows enable-period;
 flow-level-bandwidth {
 logical-interface flow-bandwidth;
 physical-interface flow-bandwidth;
 subscriber flow-bandwidth;
 }
 flow-level-control {
 logical-interface flow-control-mode;
 physical-interface flow-control-mode;
 subscriber flow-control-mode;
 }
 flow-level-detection {
 logical-interface operation-mode;
 physical-interface operation-mode;
 subscriber operation-mode;
 }
 flow-detection-mode (automatic | off | on);
 flow-recover-time recover-period;
 flow-timeout-time timeout-period;
 }
```

**Hierarchy Level** [edit system ddos-protection [protocols](#) *protocol-group packet-type* ]

**Release Information** Statement introduced in Junos OS Release 12.3.

**Description** (MX Series routers with MPCs only) Configure DDoS protection suspicious control flow detection for a packet type.

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 Flow Detection for DDoS Protection on page 33](#)

## flow-detection-mode (DDoS Flow Detection)

---

|                                 |                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | flow-detection-mode (automatic   off   on)                                                                                                                                                                                            |
| <b>Hierarchy Level</b>          | [edit system ddos-protection protocols <i>protocol-group packet-type</i> ]                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                        |
| <b>Description</b>              | (MX Series routers with MPCs only) Configure the mode of operation for flow detection for the packet type. The operation mode is effective only when flow detection is enabled.                                                       |
| <b>Default</b>                  | The default mode for all protocol groups and packet types is <b>automatic</b> .                                                                                                                                                       |
| <b>Options</b>                  | <b>automatic</b> —Detect flows only when the policer is being violated.<br><br><b>off</b> —Disable flow detection.<br><br><b>on</b> —Always monitor and detect flows, even when the policer is not being violated.                    |
| <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 Flow Detection for Individual Protocol Groups or Packets on page 40</a></li><li>• <a href="#">Configuring Flow Detection for DDoS Protection on page 33</a></li></ul> |

## flow-detect-time (DDoS Flow Detection)

|                                                                                                                                                                                                   |                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                                                                                                                                                                                     | <code>flow-detect-time seconds;</code>                                                                                                                                                                                    |
| <b>Hierarchy Level</b>                                                                                                                                                                            | [edit system ddos-protection protocols <i>protocol-group packet-type</i> <b>flow-detection</b> ]                                                                                                                          |
| <b>Release Information</b>                                                                                                                                                                        | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                            |
| <b>Description</b>                                                                                                                                                                                | (MX Series routers with MPCs only) Configure how much time must pass before a suspicious flow that has exceeded the bandwidth allowed for the packet type is confirmed to be a culprit flow.                              |
| <div>  <p><b>BEST PRACTICE:</b> We recommend that you use the default value for the detection period.</p> </div> |                                                                                                                                                                                                                           |
| <b>Options</b>                                                                                                                                                                                    | <p><b>seconds</b>—Period of excessive bandwidth required for flow to be a culprit flow.</p> <p><b>Range:</b> 1 through 60 seconds</p> <p><b>Default:</b> Three seconds</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 the Detection Period for Suspicious Flows on page 38</a></li> <li>• <a href="#">Configuring Flow Detection for DDoS Protection on page 33</a></li> </ul> |

## flow-level-bandwidth (DDoS Flow Detection)

---

|                                 |                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>flow-level-bandwidth {<br/>    logical-interface flow-bandwidth;<br/>    physical-interface flow-bandwidth;<br/>    subscriber flow-bandwidth;<br/>}</pre>                                                                        |
| <b>Hierarchy Level</b>          | [edit system ddos-protection protocols <i>protocol-group packet-type</i> ]                                                                                                                                                             |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                         |
| <b>Description</b>              | <p>(MX Series routers with MPCs only) Configure allowed flow bandwidth for the packet type at each flow aggregation level.</p> <p>The remaining statements are explained separately.</p>                                               |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                        |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 42</a></li><li>• <a href="#">Configuring Flow Detection for DDoS Protection on page 33</a></li></ul> |

## flow-level-control (DDoS Flow Detection)

---

|                                 |                                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>flow-level-control {<br/>    logical-interface flow-control-mode;<br/>    physical-interface flow-control-mode;<br/>    subscriber flow-control-mode;<br/>}</pre>                                                                                  |
| <b>Hierarchy Level</b>          | [edit system ddos-protection protocols <i>protocol-group packet-type</i> ]                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                          |
| <b>Description</b>              | <p>(MX Series routers with MPCs only) Specify how traffic in the detected flow is handled for the packet type at each flow aggregation level.</p> <p>The remaining statements are explained separately.</p>                                             |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                         |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 42</a></li><li>• <a href="#">Configuring Flow Detection for DDoS Protection on page 33</a></li></ul> |



## flow-level-detection (DDoS Flow Detection)

**Syntax**    flow-level-detection {  
                   logical-interface *flow-operation-mode*;  
                   physical-interface *flow-operation-mode*;  
                   subscriber *flow-operation-mode*;  
                   }

**Hierarchy Level**    [edit system ddos-protection protocols *protocol-group packet-type*]

**Release Information**    Statement introduced in Junos OS Release 12.3.

**Description**    (MX Series routers with MPCs only) Configure the mode of operation for flow detection for the packet type at each flow aggregation level.

The remaining statements are explained separately.



**NOTE:** Flow detection operates for individual flow aggregation levels only when the flow detection mode at the packet level is configured to either **automatic** or **on**.

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

**Related Documentation**    • [Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 40](#)  
                                          • [Configuring Flow Detection for DDoS Protection on page 33](#)

## flow-recover-time (DDoS Flow Detection)

---

|                                 |                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>flow-recover-time <i>seconds</i>;</code>                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit system ddos-protection protocols <i>protocol-group packet-type</i> ]                                                                                                                                                                            |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                        |
| <b>Description</b>              | (MX Series routers with MPCs only) Configure how much time must pass before a culprit flow for the packet type is considered to have returned to normal. The period starts when the flow drops below the threshold that triggered the last violation. |
| <b>Options</b>                  | <b><i>seconds</i></b> —Period required for the traffic to recover.<br><b>Range:</b> 1 through 3600 seconds<br><b>Default:</b> 60 seconds                                                                                                              |
| <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 the Recovery Period for a Culprit Flow on page 38</a></li><li>• <a href="#">Configuring Flow Detection for DDoS Protection on page 33</a></li></ul>                                   |

## flow-report-rate (DDoS Flow Detection)

---

|                                 |                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>flow-report-rate <i>report-rate</i>;</code>                                                                                                                                                                                                     |
| <b>Hierarchy Level</b>          | [edit system ddos-protection <a href="#">global</a> ]                                                                                                                                                                                                 |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                        |
| <b>Description</b>              | (MX Series routers with MPCs only) Set the rate at which culprit flow events are reported by system log messages, for all protocol groups and packet types on all line cards.                                                                         |
| <b>Options</b>                  | <b><i>report-rate</i></b> —Number of flows per second.<br><b>Range:</b> 1 through 50,000<br><b>Default:</b> 10                                                                                                                                        |
| <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 the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types on page 37</a></li><li>• <a href="#">Configuring Flow Detection for DDoS Protection on page 33</a></li></ul> |

## flow-timeout-time (DDoS Flow Detection)

|                                 |                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>flow-timeout-time <i>seconds</i>;</code>                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | <code>[edit system ddos-protection protocols <i>protocol-group packet-type</i>]</code>                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                        |
| <b>Description</b>              | (MX Series routers with MPCs only) Configure the period of time that a culprit flow is suppressed for the packet type. The timeout period is effective only when timing out has been enabled with the <a href="#">timeout-active-flows</a> statement. |
| <b>Options</b>                  | <p><b><i>seconds</i></b>—Period that the traffic is suppressed.</p> <p><b>Range:</b> 1 through 7200 seconds</p> <p><b>Default:</b> 300 seconds</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 the Timeout Period for a Culprit Flow on page 39</a></li> <li>• <a href="#">Configuring Flow Detection for DDoS Protection on page 33</a></li> </ul>                                 |

## fpc (DDoS)

|                                 |                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>fpc <i>slot-number</i>;   bandwidth-scale <i>percentage</i>;   burst-scale <i>percentage</i>;   disable-fpc; }</pre>                                            |
| <b>Hierarchy Level</b>          | <code>[edit system ddos-protection <a href="#">protocols</a> <i>protocol-group</i> (aggregate   <i>packet-type</i>)]</code>                                          |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.                                                                                                                       |
| <b>Description</b>              | (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Modify the DDoS policer for the packet type on the specified card.                          |
| <b>Options</b>                  | <p><b><i>slot-number</i></b>—Slot number of the card.</p> <p><b>Range:</b> Depends on the router 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>• <a href="#">Configuring DDoS Protection Policers for Individual Packet Types on page 17</a></li> </ul>                      |

## global (DDoS)

---

|                                 |                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <pre>global {<br/>  disable-fpc;<br/>  disable-logging;<br/>  disable-routing-engine;<br/>  flow-detection;<br/>  flow-report-rate;<br/>  violation-report-rate;<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit system <a href="#">ddos-protection</a> ]                                                                                                                               |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.                                                                                                                               |
| <b>Description</b>              | <p>Modify DDoS policers, event logging, and flow detection globally for all protocols.</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="#">Disabling DDoS Protection Policers and Logging Globally on page 21</a></li></ul>                                         |

## logical-interface (DDoS Flow Detection)


|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>logical-interface (<i>flow-bandwidth</i>   <i>flow-control-mode</i>   <i>flow-detection-mode</i>)</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit system ddos-protection protocols <i>protocol-group packet-type flow-level-bandwidth</i> ],<br>[edit system ddos-protection protocols <i>protocol-group packet-type flow-level-control</i> ],<br>[edit system ddos-protection protocols <i>protocol-group packet-type flow-level-detection</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Description</b>              | (MX Series routers with MPCs only) Configure flow bandwidth, flow control mode, or flow detection mode for flow detection at the logical interface flow aggregation level for the packet type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Options</b>                  | <p><b><i>flow-bandwidth</i></b>—Bandwidth for the flow at the logical interface level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type flow-level-bandwidth</i>] hierarchy level.</p> <p><b>Default:</b> 200 packets per second</p> <p><b>Range:</b> 1 through 30,000 packets per second</p> <p><b><i>flow-control-mode</i></b>—Mode for how traffic in the detected flow is controlled at the logical interface level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type flow-level-control</i>] hierarchy level.</p> <ul style="list-style-type: none"> <li>• <b>drop</b>—Drop all traffic in flow.</li> <li>• <b>keep</b>—Keep all traffic in flow.</li> <li>• <b>police</b>—Police the traffic to within its allowed bandwidth.</li> </ul> <p><b><i>flow-detection-mode</i></b>—Mode for how flow detection operates at the logical interface level when a policer has been violated. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type flow-level-detection</i>] hierarchy level.</p> <ul style="list-style-type: none"> <li>• <b>automatic</b>—Search flows at the logical interface level only when a DDoS policer is being violated and only when the flow causing the policer violation is not discovered at the finer flow aggregation level, subscriber. When the suspicious flow is not found at this level, then the search moves to a coarser level of flow aggregation (physical interface). Flows at the logical interface level are subsequently not searched again until the policer is no longer violated at the coarser level, and a subsequent violation occurs that cannot be found at the subscriber level.</li> <li>• <b>off</b>—Disable flow detection at the logical interface level so that flows are never searched at this level.</li> <li>• <b>on</b>—Search flows at the logical interface level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.</li> </ul> |
| <b>Required Privilege Level</b> | <p><b>admin</b>—To view this statement in the configuration.</p> <p><b>admin-control</b>—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

- Related Documentation**
- [Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 42](#)
  - [Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 42](#)
  - [Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 40](#)
  - [Configuring Flow Detection for DDoS Protection on page 33](#)

---

## no-flow-logging (DDoS Flow Detection)

---

|                                 |                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | no-flow-logging;                                                                                                                                                                                                                                                                                   |
| <b>Hierarchy Level</b>          | [edit system ddos-protection protocols <i>protocol-group packet-type</i> ]                                                                                                                                                                                                                         |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                                                                     |
| <b>Description</b>              | (MX Series routers with MPCs only) Disable automatic logging of flow detection culprit flow events (flow reports) for the packet type.                                                                                                                                                             |
|                                 | <div><p><b>NOTE:</b> You can disable logging of suspicious flow events (violation reports) with the <code>disable-logging</code> statement at the [edit system ddos-protection global hierarchy level].</p></div> |
| <b>Required Privilege Level</b> | admin—To view this statement in the configuration.<br>admin-control—To add this statement to the configuration.                                                                                                                                                                                    |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Disabling Automatic Logging of Culprit Flow Events for a Packet Type on page 43</a></li><li>• <a href="#">Configuring Flow Detection for DDoS Protection on page 33</a></li></ul>                                                              |

## physical-interface (DDoS Flow Detection)

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>physical-interface (flow-bandwidth   flow-control-mode   flow-detection-mode)</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Hierarchy Level</b>          | [edit system ddos-protection protocols <i>protocol-group packet-type</i> <a href="#">flow-level-bandwidth</a> ],<br>[edit system ddos-protection protocols <i>protocol-group packet-type</i> <a href="#">flow-level-control</a> ],<br>[edit system ddos-protection protocols <i>protocol-group packet-type</i> <a href="#">flow-level-detection</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>              | (MX Series routers with MPCs only) Configure flow bandwidth, flow control mode, or flow detection mode at the physical interface flow aggregation level for the packet type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Options</b>                  | <p><b><i>flow-bandwidth</i></b>—Bandwidth for the flow at the physical interface level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> <a href="#">flow-level-bandwidth</a>] hierarchy level.</p> <p><b>Default:</b> 20,000 packets per second</p> <p><b>Range:</b> 1 through 50,000 packets per second</p> <p><b><i>flow-control-mode</i></b>—Mode for how traffic in the detected flow is controlled at the physical interface level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> <a href="#">flow-level-control</a>] hierarchy level.</p> <ul style="list-style-type: none"> <li>• <b>drop</b>—Drop all traffic in flow.</li> <li>• <b>keep</b>—Keep all traffic in flow.</li> <li>• <b>police</b>—Police the traffic to within its allowed bandwidth.</li> </ul> <p><b><i>flow-detection-mode</i></b>—Mode for how flow detection operates at the physical interface level when a policer has been violated. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> <a href="#">flow-level-detection</a>] hierarchy level.</p> <ul style="list-style-type: none"> <li>• <b>automatic</b>—Search flows at the physical interface level only when a DDoS policer is being violated and only when the policer violation is not discovered at the finer aggregation levels, logical interface or subscriber. Flows at the physical interface level are subsequently not searched again until a subsequent violation occurs that cannot be found at the subscriber or logical interface levels.</li> <li>• <b>off</b>—Disable flow detection at the physical interface level so that flows are never searched at this level.</li> <li>• <b>on</b>—Search flows at the physical interface level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.</li> </ul> |
| <b>Required Privilege Level</b> | <p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

- Related Documentation**
- [Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 42](#)
  - [Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 42](#)
  - [Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 40](#)
  - [Configuring Flow Detection for DDoS Protection on page 33](#)

---

## priority (DDoS)

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>priority <i>level</i>;</code>                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hierarchy Level</b>          | [edit system ddos-protection <a href="#">protocols</a> <i>protocol-group packet-type</i> )]                                                                                                                                                                                                                                                                                                                                                |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Description</b>              | (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) 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>    | • <a href="#">Configuring DDoS Protection Policers for Individual Packet Types on page 17</a>                                                                                                                                                                                                                                                                                                                                              |



## protocols (DDoS)

```
Syntax protocols protocol-group (aggregate | packet-type) {
 bandwidth packets-per-second;
 burst size;
 bypass-aggregate;
 disable-fpc;
 disable-logging;
 disable-routing-engine;
 flow-detection-mode (automatic | off | on);
 flow-detect-time seconds;
 flow-level-bandwidth {
 logical-interface flow-bandwidth;
 physical-interface flow-bandwidth;
 subscriber flow-bandwidth;
 }
 flow-level-control {
 logical-interface flow-control-mode;
 physical-interface flow-control-mode;
 subscriber flow-control-mode;
 }
 flow-level-detection {
 logical-interface flow-operation-mode;
 physical-interface flow-operation-mode;
 subscriber flow-operation-mode;
 }
 flow-recover-time seconds;
 flow-timeout-time seconds;
 fpc slot-number {
 bandwidth-scale percentage;
 burst-scale percentage;
 disable-fpc;
 }
 no-flow-logging
 priority level;
 recover-time seconds;
 timeout-active-flows;
}
re-services {
 captive-portal {
 bandwidth packets-per-second;
 burst size;
 }
}
```

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

**Release Information** Statement introduced in Junos OS Release 11.2.

**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 to monitor all control packets within the protocol group. You can configure an aggregate policer for any protocol group.

**packet-type**—(Optional) Name of the control packet type to be policed. You can configure a specific policer for only the following packet types and protocol groups:

- **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**—DHCPDISCOVER 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**—DHCPOFFER packets.
  - **release**—DHCPRELEASE 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.
- **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:
  - **router-alert**—Router alert options packets.
  - **unclassified**— All unclassified packets in the protocol group.
- **mcast-snoop**—Control traffic for multicast snooping.
  - **igmp**—Snooped IGMP traffic.
  - **pim**—Snooped PIM control traffic.
- **mlp**—The following MLP packet types are available:
  - **aging-exception**—MLP aging exception packets.
  - **packets**—MLP packets.
  - **unclassified**—All unclassified packets in the protocol group.

- **ppp**—The following PPP packet types are available:
  - **authentication**—PPP authentication protocol packets.
  - **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.
- **tcp-flags**—The following TCP-flagged packet types are available:
  - **established**—TCP ACK and RST connection packets.
  - **initial**—TCP SYN and NAK 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.
  - **filter-v4**—Unclassified IPv4 filter action packets; sent to the host because of reject terms in firewall filters.
  - **filter-v6**—Unclassified IPv6 filter action packets; sent to the host because of reject terms in firewall filters.
  - **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.
  - **other**—All unclassified packets that do not belong to another type.
  - **resolve-v4**—Unclassified IPv4 resolve packets sent to the host because of a traffic request resolve action.
  - **resolve-v6**—Unclassified IPv6 resolve packets sent to the host because of a traffic request resolve action.
- **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***—Name of the protocol group for which traffic is policed. You can configure a policer for any of the following protocol groups:

- **amtv4**—IPv4 AMT traffic.
- **amtv6**—IPv6 AMT traffic.
- **ancp**—ANCP traffic.
- **ancpv6**—ANCPv6 traffic.
- **arp**—ARP traffic.
- **atm**—ATM traffic.
- **bfd**—BFD traffic.
- **bfdv6**—BFDv6 traffic.
- **bgp**—BGP traffic.
- **bgpv6**—BGPv6 traffic.
- **control**—Control traffic.
- **demux-autosense**—Demux autosensing traffic.
- **dhcpv4**—DHCPv4 traffic.
- **dhcpv6**—DHCPv6 traffic.
- **diameter**—Diameter and Gx-Plus traffic.
- **dns**—DNS traffic.
- **dtcp**—DTCP traffic.
- **dynamic-vlan**—Dynamic VLAN exception traffic.
- **egpv6**—EGPv6 traffic.
- **eoam**—EOAM traffic.
- **esmc**—ESMC traffic.
- **firewall-host**—Firewall send-to-host traffic.
- **frame-relay**—Frame relay traffic.
- **ftp**—FTP traffic.
- **ftpv6**—FTPv6 traffic.
- **gre**—GRE traffic.
- **icmp**—ICMP traffic.
- **igmp**—IGMP traffic.
- **igmpv4v6**—IGMP v4/v6 traffic.
- **igmpv6**—IGMPv6 traffic.
- **inline-ka**—Inline service interfaces keepalive traffic.

- **inline-svcs**—Inline services traffic.
- **ip-fragments**—IP fragments traffic.
- **ip-options**—IP traffic with IP packet header options.
- **isis**—IS-IS traffic.
- **jfm**—JFM traffic.
- **keepalive**—Keepalive traffic.
- **l2pt**—Layer 2 protocol tunneling traffic.
- **l2tp**—L2TP traffic.
- **larp**—LACP traffic.
- **ldp**—LDP traffic.
- **ldpv6**—LDPv6 traffic.
- **lldp**—LLDP traffic.
- **lmp**—LMP traffic.
- **lmpv6**—LMPv6 traffic.
- **mac-host**—Layer 2 MAC send-to-host traffic.
- **mcast-snoop**—Control traffic for multicast snooping.
- **mlp**—MLP traffic.
- **msdp**—MSDP traffic.
- **msdpv6**—MSDPv6 traffic.
- **multicast-copy**—Host copy traffic due to multicast routing.
- **mvrp**—MVRP traffic.
- **ntp**—NTP traffic.
- **oam-lfm**—OAM-LFM traffic.
- **ospf**—OSPF traffic.
- **ospfv3v6**—OSPFv3/IPv6 traffic.
- **pfe-alive**—Packet Forwarding Engine keepalive traffic.
- **pim**—PIM traffic.
- **pmvrp**—PMVRP traffic.
- **pos**—POS traffic.
- **ppp**—PPP traffic.
- **pppoe**—PPPoE traffic.
- **ptp**—PTP traffic.
- **pvstp**—PVSTP traffic.

- **radius**—RADIUS traffic.
- **redirect**—Traffic that triggers ICMP redirects.
- **reject**—Packets rejected by a next-hop forwarding decision.
- **rip**—RIP traffic.
- **ripv6**—RIPv6 traffic.
- **rsvp**—RSVP traffic.
- **rsvpv6**—RSVPv6 traffic.
- **services**—Service traffic.
- **snmp**—SNMP traffic.
- **snmpv6**—SNMPv6 traffic.
- **ssh**—SSH traffic.
- **sshv6**—SSHv6 traffic.
- **stp**—STP traffic.
- **tacacs**—TACACS traffic.
- **tcp-flags**—Traffic with TCP flags.
- **telnet**—TELNET traffic.
- **telnetv6**—TELNETv6 traffic.
- **ttl**—TTL traffic.
- **tunnel-fragment**—Tunnel fragments traffic.
- **unclassified**—Unclassified traffic.
- **virtual-chassis**—Virtual chassis traffic.
- **vrrp**—VRRP traffic.
- **vrrpv6**—VRRPv6 traffic.

The remaining statements are explained separately.

|                           |                                                           |
|---------------------------|-----------------------------------------------------------|
| <b>Required Privilege</b> | admin—To view this statement in the configuration.        |
| <b>Level</b>              | 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 on page 17</a></li></ul> |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|



---

## recover-time (DDoS)

---

|                                 |                                                                                                                                                                                                                                              |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>recover-time <i>seconds</i>;</code>                                                                                                                                                                                                    |
| <b>Hierarchy Level</b>          | [edit system ddos-protection <a href="#">protocols</a> <i>protocol-group</i> (aggregate   <i>packet-type</i> )]                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 11.2.                                                                                                                                                                                               |
| <b>Description</b>              | (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) Configure how much time must pass since the last detected DDoS violation before the traffic is considered to have recovered from the attack and returned to normal. |
| <b>Options</b>                  | <b><i>seconds</i></b> —Period required for the traffic to recover.<br><b>Range:</b> 1 through 3600 seconds<br><b>Default:</b> 300                                                                                                            |
| <b>Required Privilege Level</b> | <b>admin</b> —To view this statement in the configuration.<br><b>admin-control</b> —To add this statement to the configuration.                                                                                                              |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring DDoS Protection Policers for Individual Packet Types on page 17</a></li></ul>                                                                                                |

## subscriber (DDoS Flow Detection)

---

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | subscriber ( <i>flow-bandwidth</i>   <i>flow-control-mode</i>   <i>flow-detection-mode</i> )                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Hierarchy Level          | [edit system ddos-protection protocols <i>protocol-group packet-type flow-level-bandwidth</i> ],<br>[edit system ddos-protection protocols <i>protocol-group packet-type flow-level-control</i> ],<br>[edit system ddos-protection protocols <i>protocol-group packet-type flow-level-detection</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Release Information      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Description              | (MX Series routers with MPCs only) Configure flow bandwidth, flow control mode, or flow detection mode at the subscriber flow aggregation level for the packet type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Options                  | <p><b><i>flow-bandwidth</i></b>—Specify the bandwidth for the flow at the subscriber level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type flow-level-bandwidth</i>] hierarchy level.</p> <p><b>Default:</b> 100 packets per second</p> <p><b>Range:</b> 1 through 10,000 packets per second</p> <p><b><i>flow-control-mode</i></b>—Specify how traffic in the detected flow is controlled at the subscriber level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type flow-level-control</i>] hierarchy level.</p> <ul style="list-style-type: none"><li>• <b>drop</b>—Drop all traffic in flow.</li><li>• <b>keep</b>—Keep all traffic in flow.</li><li>• <b>police</b>—Police the traffic to within its allowed bandwidth.</li></ul> <p><b><i>flow-detection-mode</i></b>—Specify how flow detection operates at the subscriber level when a DDoS protection policer has been violated. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type flow-level-detection</i>] hierarchy level.</p> <ul style="list-style-type: none"><li>• <b>automatic</b>—Search flows at the subscriber level only when a DDoS policer is being violated and only until it is established that the flow causing the violation is not at this level. When the suspicious flow is not at this level, then the search moves to a coarser level of flow aggregation (logical interface). Flows at the subscriber level are subsequently not searched again until the policer is no longer violated at the coarser level.</li><li>• <b>off</b>—Disable flow detection at the subscriber level so that flows are never searched at this level.</li><li>• <b>on</b>—Search flows at the subscriber level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.</li></ul> |
| Required Privilege Level | 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 the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 42</a></li><li>• <a href="#">Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 42</a></li><li>• <a href="#">Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 40</a></li><li>• <a href="#">Configuring Flow Detection for DDoS Protection on page 33</a></li></ul> |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## timeout-active-flows (DDoS Flow Detection)

---

|                                 |                                                                                                                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | timeout-active-flows;                                                                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit system ddos-protection protocols <i>protocol-group packet-type</i> ]                                                                                                                                                                                                    |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                                                |
| <b>Description</b>              | (MX Series routers with MPCs only) Enable culprit flows for the packet type to time out according to the timeout period. The culprit flow is suppressed for the duration of the timeout period. When the period expires, the flow times out and is released from suppression. |
| <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 the Timeout Period for a Culprit Flow on page 39</a></li><li>• <a href="#">Configuring Flow Detection for DDoS Protection on page 33</a></li></ul>                                                            |

## traceoptions (DDoS)

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>traceoptions {<br/>    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;<br/>    &lt;world-readable   no-world-readable&gt;;<br/>    flag <i>flag</i>;<br/>    level (all   error   info   notice   verbose   warning);<br/>    no-remote-trace;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>     | [edit system <a href="#">ddos-protection</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b> | Statement introduced in Junos OS Release 11.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>         | Define tracing operations for DDoS protection processes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>             | <p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory <code>/var/log</code>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"><li>• <b>all</b>—Trace all operations.</li><li>• <b>config</b>—Trace processing of the DDoS configuration at an extensive level.</li><li>• <b>events</b>—Trace jddosd event processing; currently only exit events are traced.</li><li>• <b>gres</b>—Trace messages exchanged with the kernel and jddosd process that could affect.</li><li>• <b>init</b>—Trace jddosd initialization.</li><li>• <b>memory</b>—Trace memory management code. This flag is not currently supported.</li><li>• <b>protocol</b>—Trace DDoS protocol state processing. Only the violation state is currently traced.</li><li>• <b>rtsock</b>—Trace messages exchanged with the kernel and jddosd process.</li><li>• <b>signal</b>—Trace system signals that are passed to jddosd, such as SIGTERM.</li><li>• <b>state</b>—Trace state machine events. This flag is not currently supported.</li><li>• <b>timer</b>—Trace jddosd timer events.</li><li>• <b>ui</b>—Trace user interface processing. This flag is not currently supported.</li></ul> <p><b>level</b>—Level of tracing to perform. You can specify any of the following levels:</p> <ul style="list-style-type: none"><li>• <b>all</b>—Match all levels.</li></ul> |

- **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>• <a href="#">Tracing DDoS Protection Operations on page 133</a></li> </ul> |

## violation-report-rate (DDoS Flow Detection)

---

|                                 |                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | violation-report-rate <i>report-rate</i> ;                                                                                                                                                                                                         |
| <b>Hierarchy Level</b>          | [edit system ddos-protection <a href="#">global</a> ]                                                                                                                                                                                              |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 12.3.                                                                                                                                                                                                     |
| <b>Description</b>              | (MX Series routers with MPCs only) Limit the rate at which bandwidth violations (violation reports) are reported from an FPC to the Routing Engine, for all protocol groups and packet types on all line cards.                                    |
| <b>Options</b>                  | <b>report-rate</b> —Number of violations per second.<br><b>Range:</b> 1 through 50,000<br><b>Default:</b> 100                                                                                                                                      |
| <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 the Violation Reporting Rate for All Protocol Groups and Packet Types on page 37</a></li><li>• <a href="#">Configuring Flow Detection for DDoS Protection on page 33</a></li></ul> |

## PART 3

# Administration

- [Verifying and Monitoring Configurations on page 81](#)
- [Monitoring Commands on page 83](#)





## CHAPTER 9

# Verifying and Monitoring Configurations

- [Verifying and Managing DDoS Protection on page 81](#)
- [Verifying and Managing Flow Detection on page 82](#)

### 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 on page 82](#)
  - *Junos OS Operational Mode Commands*

---

## Verifying and Managing Flow Detection

---

**Purpose** View or clear information about flow detection as part of a DDoS protection configuration.

- Action**
- To display configuration information for flow detection:  
user@host> **show ddos-protection protocols flow-detection**
  - To display information about culprit flows identified by flow detection, including number of flows detected and tracked, source address of the flow, arriving interface, and rates:  
user@host> **show ddos-protection protocols culprit-flows**
  - To clear culprit flows for all packet types in all protocol groups:  
user@host> **clear ddos-protection protocols culprit-flows**
  - To clear culprit flows for all packet types in a particular protocol group:  
user@host> **clear ddos-protection protocols protocol-group culprit-flows**

- Related Documentation**
- [Verifying and Managing DDoS Protection on page 81](#)
  - *Junos OS Operational Mode Commands*

## CHAPTER 10

# Monitoring Commands

## clear ddos-protection protocols

---

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax                   | <code>clear ddos-protection protocols</code><br><code>&lt;protocol-group &lt;packet-type&gt;&gt; (culprit-flows   states   statistics)</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Release Information      | Command introduced in Junos OS Release 11.2.<br>Option <b>culprit-flows</b> introduced in Junos OS Release 12.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Description              | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Options                  | <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.</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> |
| Required Privilege Level | clear                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Related Documentation    | <ul style="list-style-type: none"><li>• <a href="#">show ddos-protection protocols on page 85</a></li><li>• <a href="#">show ddos-protection statistics on page 128</a></li><li>• <a href="#">show ddos-protection version on page 129</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| List of Sample Output    | <a href="#">clear ddos-protection protocols on page 84</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Output Fields            | When you enter this command, you are provided feedback on the status of your request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Sample Output

|                                              |                                                                                |
|----------------------------------------------|--------------------------------------------------------------------------------|
| <code>clear ddos-protection protocols</code> | <code>user@host&gt; clear ddos-protection protocols dhcpv4 bootp states</code> |
|----------------------------------------------|--------------------------------------------------------------------------------|

## show ddos-protection protocols

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <code>show ddos-protection protocols &lt;protocol-group (aggregate   packet-type)&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Release Information</b> | Command introduced in Junos OS Release 11.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>         | Display DDoS protection configuration and statistics for protocol groups or individual packet types.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>             | <p><b>none</b>—Display information for all packet types in all protocol groups.</p> <p><b>aggregate</b>—(Optional) Display DDoS protection information for the aggregate policer. The <b>aggregate</b> option is available for all protocol groups.</p> <p><b>packet-type</b>—(Optional) Display DDoS protection information for the specified packet type in the protocol group. The available packet types vary by protocol group. Only an aggregate policer is available for protocol groups that are not in the following list:</p> <ul style="list-style-type: none"> <li>• <b>dhcpv4</b>—The following packet types are available for DHCPv4 traffic: <ul style="list-style-type: none"> <li>• <b>ack</b>—DHCPACK packets.</li> <li>• <b>bad-packets</b>—DHCPv4 packets with bad formats.</li> <li>• <b>bootp</b>—DHCPBOOTP packets.</li> <li>• <b>decline</b>—DHCPDECLINE packets.</li> <li>• <b>discover</b>—DHCDISCOVER packets.</li> <li>• <b>force-renew</b>—DHCPFORCERENEW packets.</li> <li>• <b>inform</b>—DHCPINFORM packets.</li> <li>• <b>lease-active</b>—DHCPLEASEACTIVE packets.</li> <li>• <b>lease-query</b>—DHCPLEASEQUERY packets.</li> <li>• <b>lease-unassigned</b>—DHCPLEASEUNASSIGNED packets.</li> <li>• <b>lease-unknown</b>—DHCPLEASEUNKNOWN packets.</li> <li>• <b>nak</b>—DHCPNAK packets.</li> <li>• <b>no-message-type</b>—DHCP packets that are missing the message type..</li> <li>• <b>offer</b>—DHCOFFER packets.</li> <li>• <b>release</b>—DHCPACK packets.</li> <li>• <b>renew</b>—DHCPRENEW packets.</li> <li>• <b>request</b>—DHCPREQUEST packets.</li> <li>• <b>unclassified</b>— All unclassified packets in the protocol group.</li> </ul> </li> <li>• <b>dhcpv6</b>—The following packet types are available for DHCPv6 traffic:</li> </ul> |

- **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.
- **frame-relay**—The following packet types are available for Frame Relay traffic:
  - **frf15**—Multilink frame relay FRF.15 packets.
  - **frf16**—Multilink frame relay FRF.16 packets.
- **ip-fragments**—The following packet types are available for IP fragments:
  - **first-fragment**—First IP fragment.
  - **trail-fragment**—Last IP fragment.
- **ip-options**—The following packet types are available for IP option traffic:
  - **non-v4v6**—Options packets other than IPv4/v6.
  - **router-alert**—Router alert options packets.
  - **unclassified**— All unclassified packets in the protocol group.
- **mcast-snoop**—Control traffic for multicast snooping.
  - **igmp**—Snooped IGMP traffic.
  - **pim**—Snooped PIM control traffic.
- **mlp**—The following MLP packet types are available:

- **aging-exception**—MLP aging exception packets.
- **packets**—MLP packets.
- **unclassified**— All unclassified packets in the protocol group.
- **ppp**—The following PPP packet types are available:
  - **authentication**—PPP authentication protocol packets.
  - **echo-rep**—LCP echo reply packets.
  - **echo-req**—LCP echo request packets.
  - **ipcp**—IP Control Protocol packets.
  - **ipv6cp**—IPv6 Control Protocol packets.
  - **isis**—IS-IS packets.
  - **lcp**—Link Control Protocol packets.
  - **mlppp-lcp**—MLPPP LCP packets.
  - **mplscp**—MPLS Control Protocol packets.
  - **unclassified**— All unclassified packets in the protocol group.
- **pppoe**—The following PPPoE packet types are available:
  - **padi**—PADI packets.
  - **padm**—PADM packets.
  - **padn**—PADN packets.
  - **pado**—PADO packets.
  - **padr**—PADR packets.
  - **pads**—PADS packets.
  - **padt**—PADT packets.
- **radius**—The following RADIUS packet types are available:
  - **accounting**—RADIUS accounting packets.
  - **authorization**—RADIUS authorization packets.
  - **server**—RADIUS server traffic.
  - **unclassified**— All unclassified packets in the protocol group.
- **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.
  - **filter-v4**—Unclassified IPv4 filter action packets; sent to the host because of reject terms in firewall filters.
  - **filter-v6**—Unclassified IPv6 filter action packets; sent to the host because of reject terms in firewall filters.
  - **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.
  - **other**—All unclassified packets that do not belong to another type.
  - **resolve-v4**—Unclassified IPv4 resolve packets sent to the host because of a traffic request resolve action.
  - **resolve-v6**—Unclassified IPv6 resolve packets sent to the host because of a traffic request resolve action.
- **virtual-chassis**—The following packet types are available for virtual chassis packets:
  - **control-low**—Low-priority control packets.
  - **control-high**—High-priority control packets.
  - **unclassified**—All unclassified packets in the protocol group.
  - **vc-packets**—All exception packets on the virtual chassis link.
  - **vc-ttl-errors**—Virtual chassis TTL error packets.

***protocol-group***—(Optional) Display DDoS protection information for one of the following protocol groups:

- **amtv4**—IPv4 AMT traffic.
- **amtv6**—IPv6 AMT traffic.
- **ancp**—ANCP traffic.
- **ancpv6**—ANCPv6 traffic.
- **arp**—ARP traffic.
- **atm**—ATM traffic.



- **bfd**—BFD traffic.
- **bfdv6**—BFDv6 traffic.
- **bgp**—BGP traffic.
- **bgpv6**—BGPv6 traffic.
- **control**—Control traffic.
- **demux-autosense**—Demux autosensing traffic.
- **dhcpv4**—DHCPv4 traffic.
- **dhcpv6**—DHCPv6 traffic.
- **diameter**—Diameter and Gx-Plus traffic.
- **dns**—DNS traffic.
- **dtcp**—DTCP traffic.
- **dynamic-vlan**—Dynamic VLAN exception traffic.
- **egpv6**—EGPv6 traffic.
- **eoam**—EOAM traffic.
- **esmc**—ESMC traffic.
- **fab-probe**—Fab out probe packets.
- **firewall-host**—Firewall send-to-host traffic.
- **frame-relay**—Frame relay traffic.
- **ftp**—FTP traffic.
- **ftpv6**—FTPv6 traffic.
- **gre**—GRE traffic.
- **icmp**—ICMP traffic.
- **igmp**—IGMP traffic
- **igmpv4v6**—IGMP v4/v6 traffic.
- **igmpv6**—IGMPv6 traffic.
- **inline-ka**—Inline service interfaces keepalive traffic.
- **inline-svcs**—Inline services traffic.
- **ip-fragments**—IP fragments traffic.
- **ip-options**—IP traffic with IP packet header options.
- **isis**—IS-IS traffic.
- **jfm**—JFM traffic.
- **keepalive**—Keepalive traffic.
- **l2pt**—Layer 2 protocol tunneling traffic.

- **l2tp**—L2TP traffic.
- **lACP**—LACP traffic.
- **ldp**—LDP traffic.
- **ldpv6**—LDPv6 traffic.
- **lldp**—LLDP traffic.
- **lmp**—LMP traffic.
- **lmpv6**—LMPv6 traffic.
- **mac-host**—Layer 2 MAC send-to-host traffic.
- **mcast-snoop**—Control traffic for multicast snooping.
- **mlp**—MLP traffic.
- **msdp**—MSDP traffic.
- **msdpv6**—MSDPv6 traffic.
- **multicast-copy**—Host copy traffic due to multicast routing.
- **mvrp**—MVRP traffic.
- **ndpv6**—NDPv6 traffic.
- **ntp**—NTP traffic.
- **oam-lfm**—OAM-LFM traffic.
- **ospf**—OSPF traffic.
- **ospfv3v6**—OSPFv3/IPv6 traffic.
- **pfe-alive**—Packet Forwarding Engine keepalive traffic
- **pim**—PIM traffic.
- **pimv6**—PIMv6 traffic.
- **pmvrp**—PMVRP traffic.
- **pos**—POS traffic.
- **ppp**—PPP traffic.
- **pppoe**—PPPoE traffic.
- **ptp**—PTP traffic.
- **pvstp**—PVSTP traffic.
- **radius**—RADIUS traffic.
- **redirect**—Traffic that triggers ICMP redirects.
- **reject**—Packets rejected by a next-hop forwarding decision.
- **rejectv6**—V6 packets rejected by a next-hop forwarding decision.
- **rip**—RIP traffic.

- **ripv6**—RIPv6 traffic.
- **rsvp**—RSVP traffic.
- **rsvppv6**—RSVPv6 traffic.
- **services**—Service traffic.
- **snmp**—SNMP traffic.
- **snmpv6**—SNMPv6 traffic.
- **ssh**—SSH traffic.
- **sshv6**—SSHv6 traffic.
- **stp**—STP traffic.
- **tacacs**—TACACS traffic.
- **tcp-flags**—Traffic with TCP flags.
- **telnet**—TELNET traffic.
- **telnetv6**—TELNETv6 traffic.
- **ttl**—TTL traffic.
- **tunnel-fragment**—Tunnel fragments traffic.
- **virtual-chassis**—Virtual chassis traffic.
- **vrrp**—VRRP traffic.
- **vrrpv6**—VRRPv6 traffic.

**Required Privilege Level** view

- Related Documentation**
- [clear ddos-protection protocols on page 84](#)
  - [show ddos-protection protocols culprit-flows on page 101](#)
  - [show ddos-protection protocols flow-detection on page 104](#)
  - [show ddos-protection protocols parameters on page 108](#)
  - [show ddos-protection protocols statistics on page 115](#)
  - [show ddos-protection protocols violations on page 126](#)

- List of Sample Output**
- [show ddos-protection protocols on page 96](#)
  - [show ddos-protection protocols \(Specific Packet Type with Flow Detection Disabled\) on page 97](#)
  - [show ddos-protection protocols \(Specific Packet Type with Flow Detection Enabled and Automatic\) on page 98](#)
  - [show ddos-protection protocols \(Specific Packet Type with Bandwidth Violation\) on page 99](#)

**Output Fields** Table 5 on page 92 lists the output fields for the `show ddos-protection protocols` command. Output fields are listed in the approximate order in which they appear.

**Table 5: show ddos-protection protocols Output Fields**

| Field Name                     | Field Description                                                                                                                                                                                                                                                                |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Packet types</b>            | Number of packet types                                                                                                                                                                                                                                                           |
| <b>Modified</b>                | Number of packets for which policer values have been modified from the default.                                                                                                                                                                                                  |
| <b>Received traffic</b>        | Number of traffic flows received.                                                                                                                                                                                                                                                |
| <b>Currently violated</b>      | Number of flows that are currently violating the flow bandwidth limit.                                                                                                                                                                                                           |
| <b>Currently tracked flows</b> | Number of active flows that are being tracked as culprit flows by flow detection.                                                                                                                                                                                                |
| <b>Total detected flows</b>    | Total number of culprit flows that have been detected, including those that have recovered or timed out.                                                                                                                                                                         |
| <b>Protocol Group</b>          | Name of protocol group.                                                                                                                                                                                                                                                          |
| <b>Packet type</b>             | Name of packet type in protocol group.                                                                                                                                                                                                                                           |
| <b>Bandwidth</b>               | Bandwidth policer value; number of packets per second that is allowed before a violation is declared.                                                                                                                                                                            |
| <b>Burst</b>                   | Burst policer value; the maximum number of packets that is allowed in a burst before a violation is declared.                                                                                                                                                                    |
| <b>Priority</b>                | Priority of the packet type for individual packet policers that enables more important traffic to pass through in the event of traffic congestion: <b>low</b> , <b>medium</b> , or <b>high</b> . Lower priority packets can be dropped when insufficient bandwidth is available. |
| <b>Recover time</b>            | Time that must pass since the last violation before the traffic flow is considered to have recovered from the attack. A notification is generated when the timer expires.                                                                                                        |
| <b>Enabled</b>                 | State of the policer, enabled ( <b>Yes</b> ), disabled ( <b>No</b> ), or partially disabled ( <b>Partial</b> ); <b>Partial</b> indicates that only some of the policer instances are disabled for the policer.                                                                   |
| <b>Bypass aggregate</b>        | 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.                                        |

Table 5: show ddos-protection protocols Output Fields (*continued*)

| Field Name                          | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Flow detection configuration</b> | <p>State of flow detection configured on the router:</p> <ul style="list-style-type: none"> <li>Detection mode—Mode of operation for suspicious flow detection: automatic, off, or on.</li> <li>Log flows—State of automatic logging of suspicious traffic flows: on (<b>Yes</b>) or off (<b>No</b>).</li> <li>Timeout flows—State of culprit flow timeout behavior: flow is suppressed for a configured timeout period (<b>Yes</b>) or flow is suppressed until it is no longer in violation (<b>No</b>).</li> <li>Detect time—Time in seconds that must pass before a suspicious flow that has exceeded the bandwidth allowed for the packet type is considered to be a culprit flow.</li> <li>Recover time—Time in seconds that must pass before a culprit flow is considered to have returned to normal. The period starts when the flow drops below the threshold that triggered the last violation.</li> <li>Timeout time—Time in seconds that a culprit flow is suppressed, if timeouts have been enabled.</li> <li>Flow aggregation level configuration—Flow detection mode, flow control mode, and flow bandwidth for traffic at each of the traffic flow aggregation levels: subscriber, logical interface, and physical interface. <ul style="list-style-type: none"> <li>Detection mode—State of flow detection: automatic, off, or on.</li> <li>Control mode—Mode of controlling culprit traffic: dropped, kept, or policed back to within the allowed bandwidth.</li> <li>Flow rate—Bandwidth allowed for the control traffic in packets per second.</li> </ul> </li> </ul> |
| <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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Table 5: show ddos-protection protocols Output Fields (*continued*)

| Field Name                        | Field Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <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> |
| <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>                                                                                                                                                                                                  |

Table 5: show ddos-protection protocols Output Fields (*continued*)

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

## 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) user@host> show ddos-protection protocols pppoe padi
Currently tracked flows: 0, Total detected flows: 0
* = User configured value

```

### Packet Type with Flow Detection Disabled)

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

```

user@host> show ddos-protection protocols pppoe padi
Currently tracked flows: 0, Total detected flows: 0
* = User configured value

```

**Detection Enabled and Automatic)**

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**

```

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

```

## Packet Type with Bandwidth Violation)

\* = 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 culprit-flows

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show ddos-protection protocols &lt;protocol-group (aggregate   packet-type)&gt; culprit-flows</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release Information</b>      | Command introduced in Junos OS Release 12.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Description</b>              | Display culprit flow information for protocol groups or individual packet types.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Options</b>                  | <p><b>none</b>—Display information for all protocol groups and packet types.</p> <p><b>aggregate</b>—(Optional) Display DDoS protection information for the aggregate policer. The <b>aggregate</b> option is available for all protocol groups.</p> <p><b>packet-type</b>—(Optional) Display information for the specified packet type in the protocol group. The available packet types vary by protocol group. See <a href="#">show ddos-protection protocols</a> for a list of available packet types.</p> <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 84</a></li> <li>• <a href="#">show ddos-protection protocols on page 85</a></li> <li>• <a href="#">show ddos-protection protocols flow-detection on page 104</a></li> <li>• <a href="#">show ddos-protection protocols parameters on page 108</a></li> <li>• <a href="#">show ddos-protection protocols statistics on page 115</a></li> <li>• <a href="#">show ddos-protection protocols violations on page 126</a></li> </ul>                                                                                                                                                                    |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection protocols culprit-flows on page 102</a><br><a href="#">show ddos-protection protocols culprit-flows (Specific Protocol Group) on page 102</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Output Fields</b>            | <a href="#">Table 6 on page 101</a> lists the output fields for the <b>show ddos-protection protocols culprit-flows</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**Table 6: show ddos-protection protocols culprit-flows Output Fields**

| Field Name              | Field Description                                                                                        | Level of Output |
|-------------------------|----------------------------------------------------------------------------------------------------------|-----------------|
| Currently tracked flows | Number of active flows that are being tracked as culprit flows by flow detection.                        | none            |
| Total detected flows    | Total number of culprit flows that have been detected, including those that have recovered or timed out. | none            |
| Protocol Group          | Name of protocol group.                                                                                  | none            |

Table 6: show ddos-protection protocols culprit-flows Output Fields (*continued*)

| Field Name                          | Field Description                                                                                                                                                                                                                                                                                                      | Level of Output |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>Packet type</b>                  | Name of packet type in protocol group.                                                                                                                                                                                                                                                                                 | none            |
| <b>Arriving Interface</b>           | Logical interface on which the traffic flow arrived.                                                                                                                                                                                                                                                                   | none            |
| <b>Source Address<br/>MAC or IP</b> | Source address of the traffic flow, either a MAC address or an IP address.                                                                                                                                                                                                                                             | none            |
| <b>pps</b>                          | Rate of the traffic flow in packets per second.                                                                                                                                                                                                                                                                        | none            |
| <b>pkts</b>                         | Number of packets in the traffic flow.                                                                                                                                                                                                                                                                                 | none            |
| <b>Additional<br/>information</b>   | Flow ID numbers automatically assigned to flow, with embedded slot ID. The flow ID is prefixed by <b>sub</b> , <b>ifl</b> , or <b>ifd</b> , which indicate the subscriber, logical interface, and physical interface flow aggregation levels.<br><br>Timestamp that identifies when the flow arrived on the interface. | none            |

## Sample Output

### show ddos-protection protocols culprit-flows

```

user@host> show ddos-protection protocols culprit-flows
Currently tracked flows: 3, Total detected flows: 3

Protocol Packet Arriving Source Address
group type Interface MAC or IP
dhcpcv4 aggregate ge-1/2/0.1073741824 192.85.1.2

 sub:0001000000000000 2012-10-25 10:25:39 EDT pps:0 pkts:0
bfd aggregate ge-1/2/0.1073741824 192.85.1.2

 sub:0001000000000001 2012-10-25 10:25:39 EDT pps:30000 pkts:322137
reject aggregate ge-1/2/0.1073741824 00:10:94:00:00:02

 sub:0001000000000002 2012-10-25 10:25:39 EDT pps:0 pkts:0

```

```

root@abc> show ddos-protection protocols bfd culprit-flows
Currently tracked flows: 1, Total detected flows: 1

```

```

Protocol Packet Arriving Source Address
group type Interface MAC or IP
bfd aggregate ge-1/2/0.1073741824 192.85.1.2

 sub:0001000000000001 2012-10-25 10:25:39 EDT pps:30000 pkts:2872642

```

### show ddos-protection protocols bfd culprit-flows

```

user@host> show ddos-protection protocols bfd culprit-flows
Currently tracked flows: 1, Total detected flows: 1

```

(Specific Protocol  
Group)

| Protocol<br>group | Packet<br>type | Arriving<br>Interface | Source Address<br>MAC or IP |
|-------------------|----------------|-----------------------|-----------------------------|
| bfd               | aggregate      | ge-1/2/0.1073741824   | 192.85.1.2                  |

sub:0001000000000001 2012-10-25 10:25:39 EDT pps:30000 pkts:2872642

## show ddos-protection protocols flow-detection

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <b>Syntax</b>                   | <b>show ddos-protection protocols &lt;protocol-group&gt; flow-detection</b><br><b>&lt;brief   detail   terse&gt;</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |
| <b>Release Information</b>      | Command introduced in Junos OS Release 12.3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  |
| <b>Description</b>              | Display flow detection 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.</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 84</a></li> <li>• <a href="#">show ddos-protection protocols on page 85</a></li> <li>• <a href="#">show ddos-protection protocols culprit-flows on page 101</a></li> <li>• <a href="#">show ddos-protection protocols parameters on page 108</a></li> <li>• <a href="#">show ddos-protection protocols statistics on page 115</a></li> <li>• <a href="#">show ddos-protection protocols violations on page 126</a></li> </ul>                                                                                                                                                                                                                                                                                                          |  |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection protocols flow-detection on page 106</a><br><a href="#">show ddos-protection protocols flow-detection brief (Parameters for a Specific Protocol) on page 106</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |
| <b>Output Fields</b>            | Table 7 on page 104 lists the output fields for the <b>show ddos-protection protocols flow-detection</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |

Table 7: show ddos-protection protocols flow-detection Output Fields

| Field Name   | Field Description       | Level of Output |
|--------------|-------------------------|-----------------|
| Packet types | Number of packet types. | All levels      |



Table 7: show ddos-protection protocols flow-detection Output Fields (*continued*)

| Field Name                                  | Field Description                                                                                                                                                                                                                                                                                                                                                                | Level of Output    |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>Modified</b>                             | Number of packets for which policer values have been modified from the default.                                                                                                                                                                                                                                                                                                  | All levels         |
| <b>Protocol Group</b>                       | Name of protocol group.                                                                                                                                                                                                                                                                                                                                                          | All levels         |
| <b>Packet type</b>                          | Name of packet type in protocol group.                                                                                                                                                                                                                                                                                                                                           | All levels         |
| <b>Flow detection configuration</b>         | Configuration of flow detection at the packet level.                                                                                                                                                                                                                                                                                                                             | <b>detail none</b> |
| <b>Detection mode or Op mode</b>            | Mode of operation for flow detection at the packet level: <ul style="list-style-type: none"> <li>• <b>Automatic</b> or <b>a</b>—Search flows only when a policer is being violated.</li> <li>• <b>Off</b> or <b>x</b>—Never search flows even when a policer is being violated.</li> <li>• <b>On</b> or <b>o</b>—Search flows even when no policer is being violated.</li> </ul> | All levels         |
| <b>Policer BW (pps)</b>                     | Bandwidth allowed at the packet level.                                                                                                                                                                                                                                                                                                                                           | <b>brief terse</b> |
| <b>Detect time</b>                          | Time in seconds that a suspicious flow that has exceeded the bandwidth allowed for the packet type must remain in violation to be confirmed as a culprit flow.                                                                                                                                                                                                                   | <b>detail none</b> |
| <b>Log flows or Log flow</b>                | State of automatic logging of suspicious traffic flows for the packet type: on ( <b>Yes</b> ) or off ( <b>No</b> ).                                                                                                                                                                                                                                                              | All levels         |
| <b>Recover time</b>                         | Time in seconds that must pass before a culprit flow for the packet type is considered to have returned to normal. The period starts when the flow drops below the threshold that triggered the last violation.                                                                                                                                                                  | <b>detail none</b> |
| <b>Timeout flows or Time out</b>            | State of timeout enabling for culprit flows: <ul style="list-style-type: none"> <li>• <b>Yes</b>—Enabled; flows can time out (released from suppression) when a timeout period expires, regardless of whether flow is still in violation.</li> <li>• <b>No</b>—Disabled; flows are not allowed to time out.</li> </ul>                                                           | All levels         |
| <b>Timeout time</b>                         | Time in seconds that a culprit flow is suppressed. On expiration, the flow times out even if it is still violating the bandwidth limit.                                                                                                                                                                                                                                          | <b>detail none</b> |
| <b>Flow aggregation level configuration</b> | Configuration of flow detection for each flow aggregation level.                                                                                                                                                                                                                                                                                                                 | <b>detail none</b> |
| <b>Aggregation level or Agg level</b>       | One of three levels of flow aggregation <ul style="list-style-type: none"> <li>• <b>Subscriber</b> or <b>sub</b></li> <li>• <b>Logical interface</b> or <b>ifl</b></li> <li>• <b>Physical interface</b> or <b>ifd</b></li> </ul>                                                                                                                                                 | All levels         |
| <b>Detection mode or Op</b>                 | Mode of operation for flow detection at the flow aggregation level: <ul style="list-style-type: none"> <li>• <b>Automatic</b>—Search flows only when a policer is being violated.</li> <li>• <b>Off</b>—Never search flows even when a policer is being violated.</li> <li>• <b>On</b>—Search flows even when no policer is being violated.</li> </ul>                           | All levels         |

Table 7: show ddos-protection protocols flow-detection Output Fields (*continued*)

| Field Name                       | Field Description                                                                                                                                                                                                                                                                  | Level of Output    |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>Control mode or Fc</b>        | Mode by which traffic in a culprit flow is handled.<br><br><ul style="list-style-type: none"> <li>• <b>drop</b>—Drop all traffic in flow.</li> <li>• <b>keep</b>—Keep all traffic in flow.</li> <li>• <b>police</b>—Police the traffic to within its allowed bandwidth.</li> </ul> | All levels         |
| <b>Flow rate or BWidth (pps)</b> | Bandwidth allowed at the flow aggregation level.                                                                                                                                                                                                                                   | <b>brief terse</b> |

## Sample Output

```

show ddos-protection protocols flow-detection user@host> show ddos-protection protocols flow-detection
Packet types: 190, Modified: 2
* = User configured value

Protocol Group: IPv4-Unclassified

Packet type: aggregate
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

Protocol Group: IPv6-Unclassified

Packet type: aggregate
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

...

show ddos-protection protocols flow-detection brief user@host> show ddos-protection protocols dhcpv4 flow-detection brief
Packet types: 19, Modified: 1
* = User configured value

```

(Parameters for a  
Specific Protocol)

Detection mode(Op): a = automatic  
o = on  
x = off

Flow control mode(Fc): d = drop  
k = keep  
p = police

| Protocol<br>group | Packet<br>type | Op<br>mode | Policer<br>BW(pps) | Aggr level<br>sub | Op:Fc:BW | Width(pps)<br>ifl ifd | Log<br>flow | Time<br>out |
|-------------------|----------------|------------|--------------------|-------------------|----------|-----------------------|-------------|-------------|
| dhcpv4            | aggregate      | auto       | 5000               | a:d:10            | a:d:10   | a:d:5000              | No          | No          |
| dhcpv4            | unclass..      | auto       | 300                | a:d:10            | a:d:10   | a:d:300               | No          | No          |
| dhcpv4            | discover       | auto       | 777*               | a:d:10            | a:d:10   | a:d:500               | No          | No          |
| dhcpv4            | offer          | auto       | 1000               | a:d:10            | a:d:10   | a:d:1000              | No          | No          |
| dhcpv4            | request        | auto       | 1000               | a:d:10            | a:d:10   | a:d:1000              | No          | No          |
| dhcpv4            | decline        | auto       | 500                | a:d:10            | a:d:10   | a:d:500               | No          | No          |
| dhcpv4            | ack            | auto       | 500                | a:d:10            | a:d:10   | a:d:500               | No          | No          |
| dhcpv4            | nak            | auto       | 500                | a:d:10            | a:d:10   | a:d:500               | No          | No          |
| dhcpv4            | release        | auto       | 2000               | a:d:10            | a:d:10   | a:d:2000              | No          | No          |
| dhcpv4            | inform         | auto       | 500                | a:d:10            | a:d:10   | a:d:500               | No          | No          |
| dhcpv4            | renew          | auto       | 2000               | a:d:10            | a:d:10   | a:d:2000              | No          | No          |
| dhcpv4            | forcerenew     | auto       | 2000               | a:d:10            | a:d:10   | a:d:2000              | No          | No          |
| dhcpv4            | leasequery     | auto       | 2000               | a:d:10            | a:d:10   | a:d:2000              | No          | No          |
| dhcpv4            | leaseuna..     | auto       | 2000               | a:d:10            | a:d:10   | a:d:2000              | No          | No          |
| dhcpv4            | leaseunk..     | auto       | 2000               | a:d:10            | a:d:10   | a:d:2000              | No          | No          |
| dhcpv4            | leaseact..     | auto       | 2000               | a:d:10            | a:d:10   | a:d:2000              | No          | No          |
| dhcpv4            | bootp          | auto       | 300                | a:d:10            | a:d:10   | a:d:300               | No          | No          |
| dhcpv4            | no-msgtype     | auto       | 0                  | a:d:10            | a:d:10   | a:d:0                 | No          | No          |
| dhcpv4            | bad-pack..     | auto       | 0                  | a:d:10            | a:d:10   | a:d:0                 | No          | No          |

## show ddos-protection protocols parameters

---

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show ddos-protection protocols</b> <protocol-group> parameters<br><brief   detail   terse>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <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 84</a></li><li>• <a href="#">show ddos-protection protocols on page 85</a></li><li>• <a href="#">show ddos-protection protocols culprit-flows on page 101</a></li><li>• <a href="#">show ddos-protection protocols flow-detection on page 104</a></li><li>• <a href="#">show ddos-protection protocols statistics on page 115</a></li><li>• <a href="#">show ddos-protection protocols violations on page 126</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                          |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection protocols parameters on page 111</a><br><a href="#">show ddos-protection protocols parameters brief on page 112</a><br><a href="#">show ddos-protection protocols dhcpv4 parameters brief on page 113</a><br><a href="#">show ddos-protection protocols dhcpv4 parameters terse on page 113</a><br><a href="#">show ddos-protection protocols dhcpv4 parameters on page 113</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Output Fields</b>            | <a href="#">Table 8 on page 109</a> lists the output fields for the <b>show ddos-protection protocols parameters</b> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

Table 8: 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> |
| <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> |

Table 8: show ddos-protection protocols parameters Output Fields (*continued*)

| Field Name          | Field Description                                                                                                                                                                                                                                                                                              | Level of Output    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>Bypass aggr.</b> | 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> 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. <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<br>group | Packet<br>type | Bandwidth<br>(pps) | Burst<br>(pkts) | Priority | Recover<br>time(sec) | Policer<br>enabled | Bypass<br>aggr. | FPC<br>mod |
|-------------------|----------------|--------------------|-----------------|----------|----------------------|--------------------|-----------------|------------|
| ipv4-uncls        | aggregate      | 20000              | 20000           | medium   | 300                  | yes                | --              | no         |
| ipv6-uncls        | aggregate      | 20000              | 20000           | medium   | 300                  | yes                | --              | no         |
| dynvlan           | aggregate      | 1000               | 500             | low      | 300                  | yes                | --              | no         |
| ppp               | aggregate      | 16000              | 16000           | medium   | 300                  | yes                | --              | no         |
| ppp               | unclass        | 1000               | 500             | low      | 300                  | yes                | no              | no         |
| ppp               | lcp            | 12000              | 12000           | low      | 300                  | yes                | no              | no         |
| ppp               | auth           | 2000               | 2000            | medium   | 300                  | yes                | no              | no         |
| ppp               | ipcp           | 2000               | 2000            | high     | 300                  | yes                | no              | no         |
| ppp               | ipv6cp         | 2000               | 2000            | high     | 300                  | yes                | no              | no         |
| ppp               | mplscp         | 2000               | 2000            | high     | 300                  | yes                | no              | no         |
| ppp               | isis           | 2000               | 2000            | high     | 300                  | yes                | no              | no         |
| pppoe             | aggregate      | 800*               | 2000            | medium   | 300                  | part.*             | --              | no         |
| pppoe             | padi           | 500                | 500             | low      | 300                  | part.              | no              | no         |
| pppoe             | pado           | 0                  | 0               | low      | 300                  | part.              | no              | no         |
| pppoe             | padr           | 500                | 500             | medium   | 300                  | part.              | no              | no         |
| pppoe             | pads           | 0                  | 0               | low      | 300                  | part.              | no              | no         |
| pppoe             | padt           | 1000               | 1000            | high     | 300                  | part.              | no              | no         |
| pppoe             | padm           | 0                  | 0               | low      | 300                  | part.              | no              | no         |
| pppoe             | padn           | 0                  | 0               | low      | 300                  | part.              | no              | no         |
| dhcipv4           | aggregate      | 669*               | 5000            | medium   | 300                  | yes                | --              | no         |
| dhcipv4           | unclass..      | 300                | 150             | low      | 300                  | yes                | no              | no         |
| dhcipv4           | discover       | 100*               | 500             | low      | 300                  | yes                | no              | no         |
| dhcipv4           | offer          | 1000               | 1000            | low      | 300                  | yes                | no              | no         |
| dhcipv4           | request        | 1000               | 1000            | medium   | 300                  | yes                | no              | no         |
| dhcipv4           | decline        | 500                | 500             | low      | 300                  | yes                | no              | no         |
| dhcipv4           | ack            | 500                | 500             | medium   | 300                  | yes                | no              | no         |
| dhcipv4           | nak            | 500                | 500             | low      | 300                  | yes                | no              | no         |
| dhcipv4           | release        | 2000               | 2000            | high     | 300                  | yes                | no              | no         |
| dhcipv4           | inform         | 500                | 500             | low      | 300                  | yes                | no              | no         |
| dhcipv4           | renew          | 2000               | 2000            | high     | 300                  | yes                | no              | no         |
| dhcipv4           | forcerenew     | 2000               | 2000            | high     | 300                  | yes                | no              | no         |
| dhcipv4           | leasequery     | 2000               | 2000            | high     | 300                  | yes                | no              | no         |
| dhcipv4           | leaseuna..     | 2000               | 2000            | high     | 300                  | yes                | no              | no         |
| dhcipv4           | leaseunk..     | 2000               | 2000            | high     | 300                  | yes                | no              | no         |
| dhcipv4           | leaseact..     | 2000               | 2000            | high     | 300                  | yes                | no              | no         |
| dhcipv4           | bootp          | 300                | 300             | low      | 300                  | yes                | no              | no         |
| dhcipv4           | no-msgtype     | 0                  | 0               | low      | 300                  | yes                | no              | no         |
| dhcipv4           | bad-pack..     | 0                  | 0               | low      | 300                  | yes                | no              | no         |
| ...               |                |                    |                 |          |                      |                    |                 |            |
| icmp              | aggregate      | 20000              | 20000           | high     | 300                  | yes                | --              | no         |
| igmp              | aggregate      | 20000              | 20000           | high     | 300                  | yes                | --              | no         |



```

ospf aggregate 20000 20000 high 300 yes -- no
rsvp aggregate 20000 20000 high 300 yes -- no
pim aggregate 20000 20000 high 300 yes -- no
rip aggregate 20000 20000 high 300 yes -- no
ptp aggregate 20000 20000 high 300 yes -- no
bfd aggregate 20000 20000 high 300 yes -- no
lmp aggregate 20000 20000 high 300 yes -- no
ldp aggregate 20000 20000 high 300 yes -- no
msdp aggregate 20000 20000 high 300 yes -- no
bgp aggregate 20000 20000 low 300 yes -- no
vrrp aggregate 20000 20000 high 300 yes -- no
telnet aggregate 20000 20000 low 300 yes -- no
ftp aggregate 20000 20000 low 300 yes -- no
ssh aggregate 20000 20000 low 300 yes -- no
snmp aggregate 20000 20000 low 300 yes -- no
anycp 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>                   | <code>show ddos-protection protocols &lt;protocol-group&gt; statistics</code><br><code>&lt;brief   detail   terse&gt;</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <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 84</a></li> <li><a href="#">show ddos-protection protocols on page 85</a></li> <li><a href="#">show ddos-protection protocols culprit-flows on page 101</a></li> <li><a href="#">show ddos-protection protocols flow-detection on page 104</a></li> <li><a href="#">show ddos-protection protocols parameters on page 108</a></li> <li><a href="#">show ddos-protection protocols violations on page 126</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                             |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection protocols statistics on page 118</a><br><a href="#">show ddos-protection protocols statistics brief on page 121</a><br><a href="#">show ddos-protection protocols statistics terse on page 122</a><br><a href="#">show ddos-protection protocols pppoe statistics on page 122</a><br><a href="#">show ddos-protection protocols pppoe statistics brief on page 124</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Output Fields</b>            | <a href="#">Table 9 on page 116</a> 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 9: 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 9: 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<br>group | Packet<br>type | Received<br>(packets) | Dropped<br>(packets) | Rate<br>(pps) | Violation<br>counts | State |
|-------------------|----------------|-----------------------|----------------------|---------------|---------------------|-------|
| ipv4-unc1s        | aggregate      | 0                     | 0                    | 0             | 0                   | ok    |
| ipv6-unc1s        | aggregate      | 0                     | 0                    | 0             | 0                   | ok    |
| dynvlan           | aggregate      | 0                     | 0                    | 0             | 0                   | ok    |
| ppp               | aggregate      | 0                     | 0                    | 0             | 0                   | ok    |
| ppp               | unclass        | 0                     | 0                    | 0             | 0                   | ok    |
| ppp               | lcp            | 0                     | 0                    | 0             | 0                   | ok    |
| ppp               | auth           | 0                     | 0                    | 0             | 0                   | ok    |
| ppp               | ipcp           | 0                     | 0                    | 0             | 0                   | ok    |
| ppp               | ipv6cp         | 0                     | 0                    | 0             | 0                   | ok    |
| ppp               | mplscp         | 0                     | 0                    | 0             | 0                   | ok    |
| ppp               | isis           | 0                     | 0                    | 0             | 0                   | ok    |
| pppoe             | aggregate      | 61561238              | 0                    | 4000          | 0                   | ok    |
| pppoe             | padi           | 30780619              | 23086506             | 2000          | 1                   | viol  |
| pppoe             | pado           | 0                     | 0                    | 0             | 0                   | ok    |
| pppoe             | padr           | 30780619              | 23086499             | 2000          | 1                   | viol  |
| pppoe             | pads           | 0                     | 0                    | 0             | 0                   | ok    |
| pppoe             | padt           | 0                     | 0                    | 0             | 0                   | ok    |
| pppoe             | padm           | 0                     | 0                    | 0             | 0                   | ok    |
| pppoe             | padn           | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | aggregate      | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | unclass..      | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | discover       | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | offer          | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | request        | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | decline        | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | ack            | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | nak            | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | release        | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | inform         | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | renew          | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | forcerenew     | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | leasequery     | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | leaseuna..     | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | leaseunk..     | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | leaseact..     | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | bootp          | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | no-msgtype     | 0                     | 0                    | 0             | 0                   | ok    |
| dhcipv4           | bad-pack..     | 0                     | 0                    | 0             | 0                   | ok    |

```
...
```

|      |           |   |   |   |   |    |
|------|-----------|---|---|---|---|----|
| icmp | aggregate | 0 | 0 | 0 | 0 | ok |
| igmp | aggregate | 0 | 0 | 0 | 0 | ok |
| ospf | aggregate | 0 | 0 | 0 | 0 | ok |
| rsvp | aggregate | 0 | 0 | 0 | 0 | ok |
| pim  | aggregate | 0 | 0 | 0 | 0 | ok |
| rip  | aggregate | 0 | 0 | 0 | 0 | ok |
| ptp  | aggregate | 0 | 0 | 0 | 0 | ok |

```

bfd aggregate 0 0 0 0 ok
lmp aggregate 0 0 0 0 ok
ldp aggregate 0 0 0 0 ok
msdp aggregate 0 0 0 0 ok
bgp aggregate 0 0 0 0 ok
vrrp aggregate 0 0 0 0 ok
telnet aggregate 0 0 0 0 ok

```

```
...
```

#### show ddos-protection protocols statistics terse

```

user@host> show ddos-protection protocols statistics terse
Protocol Packet Received Dropped Rate Violation State
group type (packets) (packets) (pps) counts
ipv4-uncles 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
lisp aggregate 1744 0 0 0 ok
stp aggregate 9791 0 0 0 ok
arp aggregate 19 0 0 0 ok
pvstp aggregate 393 0 0 0 ok
mlp aggregate 624774 0 0 0 ok
mlp packets 1714371 223937 0 3 ok
mcast-copy aggregate 3018038 0 0 0 ok
igmp-snoop aggregate 43 0 0 0 ok
fw-host aggregate 95547 0 0 0 ok
uncles 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**user@host> **show ddos-protection protocols pppoe statistics brief**

| Protocol | Packet | Received | Dropped | Rate | Violation State |
|----------|--------|----------|---------|------|-----------------|
|----------|--------|----------|---------|------|-----------------|

protocols pppoe  
statistics brief

| group | type      | (packets) | (packets) | (pps) | counts |      |
|-------|-----------|-----------|-----------|-------|--------|------|
| pppoe | aggregate | 60901227  | 0         | 4000  | 0      | ok   |
| pppoe | padi      | 30450613  | 22838981  | 2000  | 1      | viol |
| pppoe | pado      | 0         | 0         | 0     | 0      | ok   |
| pppoe | padr      | 30450614  | 22838977  | 2000  | 1      | viol |
| pppoe | pads      | 0         | 0         | 0     | 0      | ok   |
| pppoe | padt      | 0         | 0         | 0     | 0      | ok   |
| pppoe | padm      | 0         | 0         | 0     | 0      | ok   |
| pppoe | padn      | 0         | 0         | 0     | 0      | ok   |

## show ddos-protection protocols violations

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <code>show ddos-protection protocols &lt;protocol-group&gt; violations</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <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 84</a></li> <li>• <a href="#">show ddos-protection protocols on page 85</a></li> <li>• <a href="#">show ddos-protection protocols culprit-flows on page 101</a></li> <li>• <a href="#">show ddos-protection protocols flow-detection on page 104</a></li> <li>• <a href="#">show ddos-protection protocols parameters on page 108</a></li> <li>• <a href="#">show ddos-protection protocols statistics on page 115</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection protocols violations on page 127</a><br><a href="#">show ddos-protection protocols dhcpv4 violations on page 127</a><br><a href="#">show ddos-protection protocols pppoe violations on page 127</a>                                                                                                                                                                                                                                                                                           |
| <b>Output Fields</b>            | <a href="#">Table 10 on page 126</a> lists the output fields for the <code>show ddos-protection protocols violations</code> command. Output fields are listed in the approximate order in which they appear.                                                                                                                                                                                                                                                                                                                   |

Table 10: 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                                                                      |
| Arrival rate (pps)                             | Current traffic rate for packets arriving from all cards and at the Routing Engine     |
| Peak rate (pps)                                | Highest traffic rate for packets arriving from all cards and at the Routing Engine     |

Table 10: show ddos-protection protocols violations Output Fields (*continued*)

| Field Name                              | Field Description                                           |
|-----------------------------------------|-------------------------------------------------------------|
| Policer bandwidth violation detected at | Timestamp of the policer violation                          |
| Detected on                             | 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 dhcpv4 violations

```
user@host> show ddos-protection protocols dhcpv4 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
```

## show ddos-protection statistics

|                                 |                                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show ddos-protection statistics</b>                                                                                                                                                                                                                  |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.2.                                                                                                                                                                                                            |
| <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 84</a></li> <li>• <a href="#">show ddos-protection protocols on page 85</a></li> <li>• <a href="#">show ddos-protection version on page 129</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection statistics on page 128</a>                                                                                                                                                                                             |
| <b>Output Fields</b>            | <a href="#">Table 11 on page 128</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 11: show ddos-protection statistics Output Fields**

| Field Name                        | Field Description                                                                                 |
|-----------------------------------|---------------------------------------------------------------------------------------------------|
| Currently violated packet types   | Number of packet types currently experiencing a bandwidth violation.                              |
| Packet types have seen violations | Number of packet types that have experienced a bandwidth violation since statistics were cleared. |
| Total violation counts            | Total number of bandwidth violations.                                                             |

## Sample Output

```

show ddos-protection statistics user@host> show ddos-protection statistics
DDOS protection global statistics:
 Currently violated packet types: 2
 Packet types have seen violations: 2
 Total violation counts: 2

```



## show ddos-protection version

|                                 |                                                                                                                                                                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>                   | <b>show ddos-protection version</b>                                                                                                                                                                                                                        |
| <b>Release Information</b>      | Command introduced in Junos OS Release 11.2.                                                                                                                                                                                                               |
| <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 84</a></li> <li>• <a href="#">show ddos-protection protocols on page 85</a></li> <li>• <a href="#">show ddos-protection statistics on page 128</a></li> </ul> |
| <b>List of Sample Output</b>    | <a href="#">show ddos-protection version on page 129</a>                                                                                                                                                                                                   |
| <b>Output Fields</b>            | Table 12 on page 129 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 12: 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

```



## PART 4

# Troubleshooting

- [Acquiring Troubleshooting Information on page 133](#)
- [Troubleshooting Configuration Statements on page 139](#)



# Acquiring Troubleshooting Information

- [Tracing DDoS Protection Operations on page 133](#)
- [Configuring the DDoS Protection Trace Log Filename on page 134](#)
- [Configuring the Number and Size of DDoS Protection Log Files on page 134](#)
- [Configuring Access to the DDoS Protection Log File on page 135](#)
- [Configuring a Regular Expression for DDoS Protection Messages to Be Logged on page 135](#)
- [Configuring the DDoS Protection Tracing Flags on page 136](#)
- [Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged on page 136](#)
- [Collecting Subscriber Access Logs Before Contacting Juniper Technical Support on page 136](#)

## 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 **ddosd**. 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.

To configure all aspects of DDoS tracing operations:

1. (Optional) Configure a trace log filename.  
See [“Configuring the DDoS Protection Trace Log Filename” on page 134](#).
2. (Optional) Configure the number and size of trace logs.  
See [“Configuring the Number and Size of DDoS Protection Log Files” on page 134](#).
3. (Optional) Configure user access to trace logs.  
See [“Configuring Access to the DDoS Protection Log File” on page 135](#).
4. (Optional) Configure a regular expression to filter the information to be included in the trace log.  
See [“Configuring a Regular Expression for DDoS Protection Messages to Be Logged” on page 135](#).
5. (Optional) Configure flags to specify which events are logged.  
See [“Configuring the DDoS Protection Tracing Flags” on page 136](#).
6. (Optional) Configure a severity level for messages to specify which event messages are logged.  
See [“Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged” on page 136](#).

**Related Documentation** • [Example: Configuring DDoS Protection on page 23](#)

---

## Configuring the DDoS Protection Trace Log Filename

By default, the name of the file that records trace output for DDoS protection is **ddosd**. You can specify a different name with the **file** option.

To configure the filename for subscriber management database tracing operations:

- Specify the name of the file used for the trace output.  

```
[edit system ddos-protection traceoptions]
user@host# set file ddos_logfile_1
```

**Related Documentation** • [Tracing DDoS Protection Operations on page 133](#)

---

## 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
```

#### Related Documentation

- [Tracing DDoS Protection Operations on page 133](#)

## 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
```

#### Related Documentation

- [Tracing DDoS Protection Operations on page 133](#)

## 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
```

**Related  
Documentation**

- [Tracing DDoS Protection Operations on page 133](#)

---

## 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
```

**Related  
Documentation**

- [Tracing DDoS Protection Operations on page 133](#)

---

## 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**

- [Tracing DDoS Protection Operations on page 133](#)

---

## Collecting Subscriber Access Logs Before Contacting Juniper Technical Support

**Problem** When you experience a subscriber access problem in your network, we recommend that you collect certain logs before you contact Juniper Technical Support. This topic shows you the most useful logs for a variety of network implementations. In addition to the



relevant log information, you must also collect standard troubleshooting information and send it to Juniper Technical Support in your request for assistance.

**Solution** To collect standard troubleshooting information:

- Redirect the command output to a file.

```
user@host> request support information | save rsi-1
```

To configure logging to assist Juniper Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.

```
[edit]
set system syslog archive size 100m files 25
set system auto-configuration traceoptions file filename
set system auto-configuration traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions level all
set protocols ppp-service traceoptions flag all
set protocols ppp traceoptions file filename size 100m files 25
set protocols ppp traceoptions level all
set protocols ppp traceoptions flag all
set protocols ppp monitor-session all
set interfaces pp0 traceoptions flag all
set demux traceoptions file filename size 100m files 25
set demux traceoptions level all
set demux traceoptions flag all
set system processes dhcp-service traceoptions file filename
set system processes dhcp-service traceoptions file size 100m
set system processes dhcp-service traceoptions file files 25
set system processes dhcp-service traceoptions flag all
set class-of-service traceoptions file filename
set class-of-service traceoptions file size 100m
set class-of-service traceoptions flag all
set class-of-service traceoptions file files 25
set routing-options traceoptions file filename
set routing-options traceoptions file size 100m
set routing-options traceoptions flag all
set routing-options traceoptions file files 25
set interfaces traceoptions file filename
set interfaces traceoptions file size 100m
set interfaces traceoptions flag all
set interfaces traceoptions file files 25
set system processes general-authentication-service traceoptions file filename
set system processes general-authentication-service traceoptions file size 100m
set system processes general-authentication-service traceoptions flag all
set system processes general-authentication-service traceoptions file files 25
```

2. Copy the relevant statements into a text file and modify the log filenames as you want.
3. Copy the statements from the text file and paste them into the CLI on your router to configure logging.
4. Commit the logging configuration to begin collecting information.



.....

**NOTE:** The maximum file size for DHCP local server and DHCP relay log files is 1 GB. The maximum number of log files for DHCP local server and DHCP relay is 1000.

.....



.....

**BEST PRACTICE:** Enable these logs only to collect information when troubleshooting specific problems. Enabling these logs during normal operations can result in reduced system performance.

.....

**Related  
Documentation**

- *Compressing Troubleshooting Logs from /var/logs to Send to Juniper Technical Support*

## CHAPTER 12

# Troubleshooting Configuration Statements

## traceoptions (DDoS)

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax</b>              | <pre>traceoptions {<br/>    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;<br/>    &lt;world-readable   no-world-readable&gt;;<br/>    flag <i>flag</i>;<br/>    level (all   error   info   notice   verbose   warning);<br/>    no-remote-trace;<br/>}</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Hierarchy Level</b>     | [edit system <a href="#">ddos-protection</a> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Release Information</b> | Statement introduced in Junos OS Release 11.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>         | Define tracing operations for DDoS protection processes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Options</b>             | <p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory <code>/var/log</code>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"><li>• <b>all</b>—Trace all operations.</li><li>• <b>config</b>—Trace processing of the DDoS configuration at an extensive level.</li><li>• <b>events</b>—Trace jddosd event processing; currently only exit events are traced.</li><li>• <b>gres</b>—Trace messages exchanged with the kernel and jddosd process that could affect.</li><li>• <b>init</b>—Trace jddosd initialization.</li><li>• <b>memory</b>—Trace memory management code. This flag is not currently supported.</li><li>• <b>protocol</b>—Trace DDoS protocol state processing. Only the violation state is currently traced.</li><li>• <b>rtsock</b>—Trace messages exchanged with the kernel and jddosd process.</li><li>• <b>signal</b>—Trace system signals that are passed to jddosd, such as SIGTERM.</li><li>• <b>state</b>—Trace state machine events. This flag is not currently supported.</li><li>• <b>timer</b>—Trace jddosd timer events.</li><li>• <b>ui</b>—Trace user interface processing. This flag is not currently supported.</li></ul> <p><b>level</b>—Level of tracing to perform. You can specify any of the following levels:</p> <ul style="list-style-type: none"><li>• <b>all</b>—Match all levels.</li></ul> |

- **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>• <a href="#">Tracing DDoS Protection Operations on page 133</a></li> </ul> |



## PART 5

# Index

- [Index on page 145](#)





# Index

## Symbols

|                                              |     |
|----------------------------------------------|-----|
| #, comments in configuration statements..... | xiv |
| ( ), in syntax descriptions.....             | xiv |
| < >, in syntax descriptions.....             | xiv |
| [ ], in configuration statements.....        | xiv |
| { }, in configuration statements.....        | xiv |
| (pipe), in syntax descriptions.....          | xiv |

## B

|                                          |     |
|------------------------------------------|-----|
| bandwidth statement                      |     |
| DDoS protection.....                     | 46  |
| bandwidth-scale statement                |     |
| DDoS protection.....                     | 47  |
| braces, in configuration statements..... | xiv |
| brackets                                 |     |
| angle, in syntax descriptions.....       | xiv |
| square, in configuration statements..... | xiv |
| burst statement                          |     |
| DDoS protection.....                     | 47  |
| burst-scale statement                    |     |
| DDoS protection.....                     | 48  |
| bypass-aggregate statement               |     |
| DDoS protection.....                     | 48  |

## C

|                                                |      |
|------------------------------------------------|------|
| clear ddos-protection protocols command.....   | 84   |
| comments, in configuration statements.....     | xiv  |
| conventions                                    |      |
| text and syntax.....                           | xiii |
| curly braces, in configuration statements..... | xiv  |
| customer support.....                          | xv   |
| contacting JTAC.....                           | xv   |

## D

|                                              |     |
|----------------------------------------------|-----|
| DDoS protection                              |     |
| clearing statistics and violations.....      | 84  |
| configuration example.....                   | 23  |
| configuration overview.....                  | 15  |
| culprit flow information, displaying.....    | 101 |
| disabling policers and logging globally..... | 21  |
| flags for tracing operations.....            | 136 |

|                                                  |        |
|--------------------------------------------------|--------|
| flow-detection information, displaying.....      | 104    |
| log file access for tracing operations.....      | 135    |
| log file size and number.....                    | 134    |
| log filenames.....                               | 134    |
| logging                                          |        |
| disabling globally.....                          | 21     |
| message severity levels for tracing              |        |
| operations.....                                  | 136    |
| overview.....                                    | 3      |
| packet-level configuration.....                  | 17     |
| policers                                         |        |
| aggregate.....                                   | 4      |
| disabling globally.....                          | 21     |
| disabling individual.....                        | 17     |
| hierarchy.....                                   | 5      |
| packet-level configuration.....                  | 17     |
| protocol.....                                    | 4      |
| scaling.....                                     | 5      |
| protocol information, displaying.....            | 85     |
| protocol policer information, displaying.....    | 108    |
| protocol policer violation information,          |        |
| displaying.....                                  | 126    |
| protocol statistics information, displaying..... | 115    |
| regular expressions for tracing operations.....  | 135    |
| statistics, displaying.....                      | 128    |
| suspicious control flow detection.....           | 9      |
| tracing operations.....                          | 133    |
| traffic priority                                 |        |
| aggregate.....                                   | 4      |
| verifying configuration.....                     | 81     |
| version, displaying.....                         | 129    |
| DDoS protection flow detection                   |        |
| configuration overview.....                      | 33, 35 |
| DDoS protection statements                       |        |
| bandwidth.....                                   | 46     |
| bandwidth-scale.....                             | 47     |
| burst.....                                       | 47     |
| burst-scale.....                                 | 48     |
| bypass-aggregate.....                            | 48     |
| ddos-protection.....                             | 49     |
| disable-fpc.....                                 | 50     |
| disable-logging.....                             | 51     |
| disable-routing-engine.....                      | 51     |
| flow-detect-time.....                            | 55     |
| flow-detection.....                              | 52, 53 |
| flow-detection-mode.....                         | 54     |
| flow-level-bandwidth.....                        | 56     |
| flow-level-control.....                          | 56     |
| flow-level-detection.....                        | 57     |

|                                                   |         |                                               |        |
|---------------------------------------------------|---------|-----------------------------------------------|--------|
| flow-recover-time.....                            | 58      | global rate for reporting violations.....     | 37     |
| flow-report-rate.....                             | 58      | verifying configuration.....                  | 82     |
| flow-timeout-time.....                            | 59      | flow detection, DDoS protection statements    |        |
| fpc.....                                          | 59      | flow-detect-time.....                         | 55     |
| global.....                                       | 60      | flow-detection.....                           | 52, 53 |
| logical-interface.....                            | 61      | flow-detection-mode.....                      | 54     |
| no-flow-logging.....                              | 62      | flow-level-bandwidth.....                     | 56     |
| physical-interface.....                           | 63      | flow-level-control.....                       | 56     |
| priority.....                                     | 64      | flow-level-detection.....                     | 57     |
| protocols.....                                    | 65      | flow-recover-time.....                        | 58     |
| recover-time.....                                 | 73      | flow-report-rate.....                         | 58     |
| subscriber.....                                   | 74      | flow-timeout-time.....                        | 59     |
| timeout-active-flows.....                         | 75      | logical-interface.....                        | 61     |
| traceoptions.....                                 | 76, 140 | no-flow-logging.....                          | 62     |
| violation-report-rate.....                        | 78      | physical-interface.....                       | 63     |
| ddos-protection statement                         |         | subscriber.....                               | 74     |
| DDoS protection.....                              | 49      | timeout-active-flows.....                     | 75     |
| denial-of-service attacks                         |         | violation-report-rate.....                    | 78     |
| protecting against See DDoS Protection            |         | flow-detect-time statement                    |        |
| disable-fpc statement                             |         | DDoS protection flow detection.....           | 55     |
| DDoS protection.....                              | 50      | flow-detection statement                      |        |
| disable-logging statement                         |         | DDoS protection flow detection.....           | 52, 53 |
| DDoS protection.....                              | 51      | flow-detection-mode statement                 |        |
| disable-routing-engine statement                  |         | DDoS protection flow detection.....           | 54     |
| DDoS protection.....                              | 51      | flow-level-bandwidth statement                |        |
| distributed denial-of-service See DDoS protection |         | DDoS protection flow detection.....           | 56     |
| documentation                                     |         | flow-level-control statement                  |        |
| comments on.....                                  | xv      | DDoS protection flow detection.....           | 56     |
| <b>E</b>                                          |         | flow-level-detection statement                |        |
| enable-timeout-active statement                   |         | DDoS protection flow detection.....           | 57     |
| DDoS protection flow detection.....               | 75      | flow-recover-time statement                   |        |
| <b>F</b>                                          |         | DDoS protection flow detection.....           | 58     |
| flow detection See overview                       |         | flow-report-rate statement                    |        |
| flow detection, DDoS protection                   |         | DDoS protection flow detection.....           | 58     |
| configuration overview.....                       | 33, 35  | flow-timeout-time statement                   |        |
| configuring the detection period.....             | 38      | DDoS protection flow detection.....           | 59     |
| configuring the flow bandwidth.....               | 42      | font conventions.....                         | xiii   |
| configuring the flow control mode.....            | 42      | fpc statement                                 |        |
| configuring the flow operation mode.....          | 40      | DDoS protection.....                          | 59     |
| configuring the operation mode.....               | 40      | <b>G</b>                                      |        |
| configuring the recovery period.....              | 38      | global statement                              |        |
| configuring the timeout period.....               | 39      | DDoS protection.....                          | 60     |
| disabling automatic logging for packet            |         | <b>L</b>                                      |        |
| types.....                                        | 43      | log files                                     |        |
| enabling flow detection globally.....             | 37      | collecting for Juniper Technical Support..... | 136    |
| global rate for reporting suspicious flows.....   | 37      | filenames for DDoS protection.....            | 134    |

- number of DDoS protection.....134
  - size of DDoS protection.....134
- logical-interface statement
  - DDoS protection flow detection.....61
- M**
- manuals
  - comments on.....xv
- N**
- no-flow-logging statement
  - DDoS protection flow detection.....62
- P**
- parentheses, in syntax descriptions.....xiv
- physical-interface statement
  - DDoS protection flow detection.....63
- priority statement
  - DDoS protection.....64
- protocols statement
  - DDoS protection.....65
- R**
- recover-time statement
  - DDoS protection.....73
- S**
- show ddos-protection protocols
  - command.....85, 104
- show ddos-protection protocols culprit-flows
  - command.....101
- show ddos-protection protocols parameters
  - command.....108
- show ddos-protection protocols statistics
  - command.....115
- show ddos-protection protocols violations
  - command.....126
- show ddos-protection statistics command.....128
- show ddos-protection version command.....129
- subscriber statement
  - DDoS protection flow detection.....74
- support, technical See technical support
- suspicious control flow detection See flow detection
- suspicious flows
  - detection period for culprit flows.....38
  - disabling automatic logging for packet
    - types.....43
  - enabling detection globally.....37
  - flow bandwidth.....42
  - flow control mode .....42
  - flow operation mode .....40
  - global reporting rate.....37
  - global reporting rate for violations.....37
  - operation mode .....40
  - recovery period for culprit flows.....38
  - timeout period for culprit flows.....39
- syntax conventions.....xiii
- T**
- technical support
  - collecting logs for.....136
  - contacting JTAC.....xv
- trace operations
  - collecting logs for Juniper technical
    - support.....136
- traceoptions statement
  - DDoS protection.....76, 140
- tracing operations
  - DDoS protection.....133
- troubleshooting subscriber access
  - collecting logs for Juniper Technical
    - Support.....136
- V**
- violation-report-rate statement
  - DDoS protection flow detection.....78

