



Junos[®] OS

DDoS Protection Configuration Guide

Release
12.1



Published: 2012-02-29

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 DDoS Protection Configuration Guide

Copyright © 2012, Juniper Networks, Inc.
All rights reserved.

Revision History
March 2012—R1 Junos OS 12.1

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.

Abbreviated Table of Contents

Part 1	Distributed Denial-of-Service (DDoS) Protection	
Chapter 1	DDoS Overview	3
Chapter 2	Configuring DDoS Protection	9
Chapter 3	DDoS Protection Configuration Hierarchy	29
Chapter 4	DDoS Protection Configuration Statements	31
Part 2	Indexes	
	Index	51
	Index of Statements and Commands	53

Table of Contents

Part 1	Distributed Denial-of-Service (DDoS) Protection	
Chapter 1	DDoS Overview	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	Configuring DDoS Protection	9
	Configuring Protection Against DDoS Attacks	9
	Disabling DDoS Protection Policers and Logging Globally	10
	Configuring DDoS Protection Policers for Individual Packet Types	10
	Tracing DDoS Protection Operations	13
	Configuring the DDoS Protection Trace Log Filename	14
	Configuring the Number and Size of DDoS Protection Log Files	14
	Configuring Access to the DDoS Protection Log File	15
	Configuring a Regular Expression for DDoS Protection Messages to Be Logged	15
	Configuring the DDoS Protection Tracing Flags	16
	Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged	16
	Verifying and Managing DDoS Protection	16
	Example: Configuring DDoS Protection	17
Chapter 3	DDoS Protection Configuration Hierarchy	29
	[edit system ddos-protection] Hierarchy Level	29
Chapter 4	DDoS Protection Configuration Statements	31
	bandwidth (DDoS)	31
	bandwidth-scale (DDoS)	32
	burst (DDoS)	32
	burst-scale (DDoS)	33
	bypass-aggregate (DDoS)	33
	ddos-protection (DDoS)	34
	disable-fpc (DDoS)	35
	disable-logging (DDoS)	35
	disable-routing-engine (DDoS)	36
	fpc (DDoS)	36
	global (DDoS)	37
	priority (DDoS)	37
	protocols (DDoS)	38

recover-time (DDoS) 45

traceoptions (DDoS) 46

Part 2

Indexes

Index 51

Index of Statements and Commands 53

List of Figures

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

PART 1

Distributed Denial-of-Service (DDoS) Protection

- [DDoS Overview on page 3](#)
- [Configuring DDoS Protection on page 9](#)
- [DDoS Protection Configuration Hierarchy on page 29](#)
- [DDoS Protection Configuration Statements on page 31](#)

CHAPTER 1

DDoS Overview

- [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 Trio MPC 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 consider 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 Trio MPCs installed. If the router has other line cards in addition to Trio MPCs, 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 Trio 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

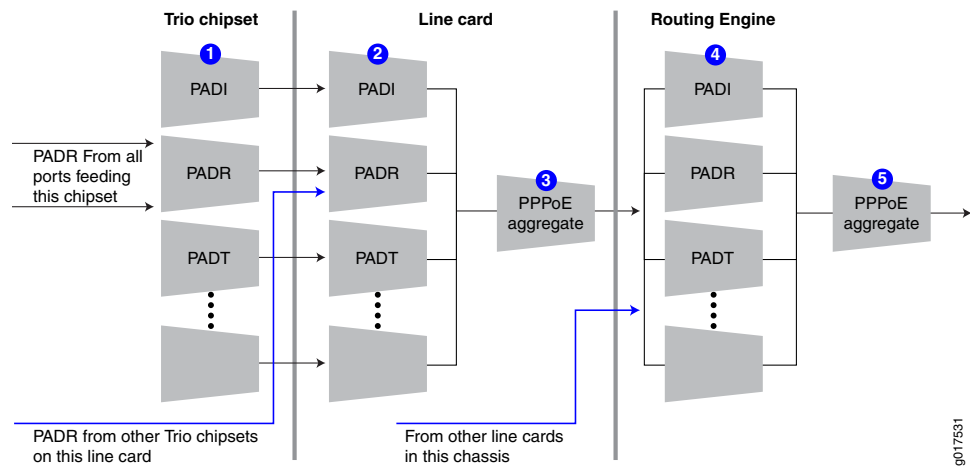
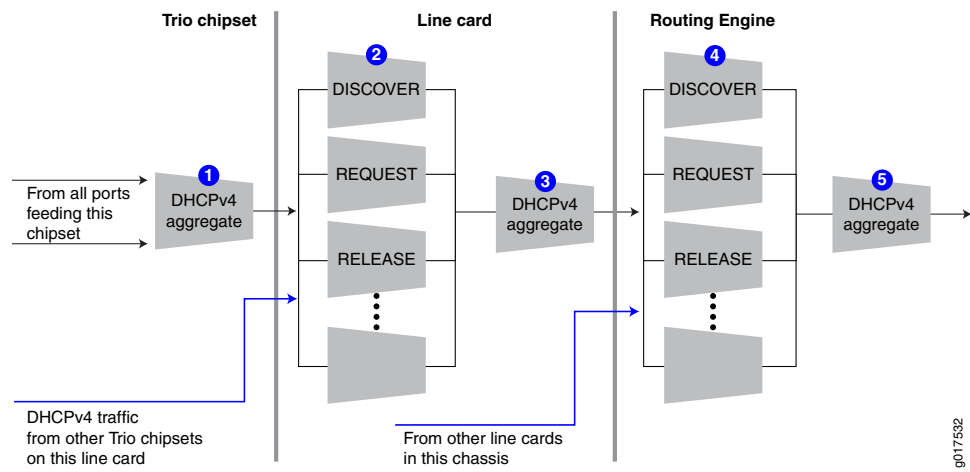


Figure 2: Policer Hierarchy for DHCPv4 Packets



Control packets arrive at the Trio chipset on the MPC 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 Trio chipset, traffic from all Trio 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 Trio MPCs 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 Trio 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 Trio chipsets on the Trio MPC 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 Trio MPCs 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 (Trio 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 Trio 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 9](#)

CHAPTER 2

Configuring DDoS Protection

- [Configuring Protection Against DDoS Attacks on page 9](#)
- [Disabling DDoS Protection Policers and Logging Globally on page 10](#)
- [Configuring DDoS Protection Policers for Individual Packet Types on page 10](#)
- [Tracing DDoS Protection Operations on page 13](#)
- [Configuring the DDoS Protection Trace Log Filename on page 14](#)
- [Configuring the Number and Size of DDoS Protection Log Files on page 14](#)
- [Configuring Access to the DDoS Protection Log File on page 15](#)
- [Configuring a Regular Expression for DDoS Protection Messages to Be Logged on page 15](#)
- [Configuring the DDoS Protection Tracing Flags on page 16](#)
- [Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged on page 16](#)
- [Verifying and Managing DDoS Protection on page 16](#)
- [Example: Configuring DDoS Protection on page 17](#)

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 Trio MPCs installed. If the router has other line cards in addition to Trio MPCs, 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 10.
2. (Optional) Configure DDoS settings for individual packet types.
See [“Configuring DDoS Protection Policers for Individual Packet Types”](#) on page 10.
3. (Optional) Configure tracing for DDoS operations.
See [“Tracing DDoS Protection Operations”](#) on page 13.

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 Trio MPCs. 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 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 9

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# set protocol-group
```

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
```

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
```

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
```

5. (Optional) Set the traffic priority.

```
[edit system ddos-protection protocols protocol-group packet-type]
```

user@host# **set** *priority level*

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*

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*

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.

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: 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.

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.

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*

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
```

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
```

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
```

- Related Documentation**
- [Configuring Protection Against DDoS Attacks on page 9](#)
 - For a list of supported protocol groups and packet types, see [protocols on page 38](#).

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 14](#).
2. (Optional) Configure the number and size of trace logs.
See [“Configuring the Number and Size of DDoS Protection Log Files” on page 14](#).

3. (Optional) Configure user access to trace logs.
See [“Configuring Access to the DDoS Protection Log File” on page 15.](#)
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 15.](#)
5. (Optional) Configure flags to specify which events are logged.
See [“Configuring the DDoS Protection Tracing Flags” on page 16.](#)
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 16.](#)

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 13](#)

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 13](#)

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 13](#)

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 13](#)

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 13](#)

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 13](#)

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 statistics protocol-group`
- To clear DDoS statistics for a particular packet type in a particular protocol group:
`user@host> clear ddos-protection protocols statistics protocol-group packet-type`
- To clear DDoS violation states for all packet types in all protocol groups:
`user@host> clear ddos-protection protocols state`
- To clear DDoS violation states for all packet types in a particular protocol group:
`user@host> clear ddos-protection protocols state protocol-group`
- To clear DDoS violation states for a particular packet type in a particular protocol group:
`user@host> clear ddos-protection protocols state protocol-group packet-type`

**Related
Documentation**

- [Junos OS System Basics and Services Command Reference](#)

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 18](#)
- [Overview on page 18](#)
- [Configuration on page 18](#)
- [Verification on page 21](#)

Requirements

DDoS protection requires the following hardware and software:

- MX Series 3D Universal Edge Routers that have only Trio MPCs installed.



NOTE: If the router has other cards in addition to Trio MPCs, 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# set 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 Trio MPC 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 21](#)
- [Verifying the PPPoE DDoS Configuration on page 24](#)

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 DHCPOFFER)
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 9](#)

CHAPTER 3

DDoS Protection Configuration Hierarchy

- [\[edit system ddos-protection\] Hierarchy Level on page 29](#)

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

```
system {
  ddos-protection {
    global {
      disable-fpc;
      disable-logging;
      disable-routing-engine;
    }
    protocols protocol-group (aggregate | packet-type) {
      bandwidth packets-per-second;
      burst size;
      bypass-aggregate;
      disable-fpc;
      disable-logging;
      disable-routing-engine;
      fpc slot-number {
        bandwidth-scale percentage;
        burst-scale percentage;
        disable-fpc;
      }
      priority level;
      recover-time seconds;
    }
    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 9](#)

CHAPTER 4

DDoS Protection Configuration Statements

bandwidth (DDoS)

Syntax	<code>bandwidth <i>packets-per-second</i>;</code>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	(MX Series routers with Trio MPCs only) 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.
Options	<i>packets-per-second</i> —Number of packets per second that are allowed for the packet type. Range: 1 through 100,000 packets per second
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring DDoS Protection Policers for Individual Packet Types on page 10

bandwidth-scale (DDoS)

Syntax	<code>bandwidth-scale <i>percentage</i>;</code>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>) fpc <i>slot-number</i>]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	(MX Series routers with Trio MPCs only) Configure the percentage by which the DDoS bandwidth rate limit is scaled down for the packet type on the card in the specified slot.
Options	<i>percentage</i> —Percentage multiplied by the bandwidth rate limit to reduce the number of packets per second allowed for the packet type. Range: 1 through 100 percent Default: 100
Required Privilege Level	admin —To view this statement in the configuration. admin-control —To add this statement to the configuration.

burst (DDoS)

Syntax	<code>burst <i>size</i>;</code>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	(MX Series routers with Trio MPCs only) 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.
Options	<i>size</i> —Number of packets that are allowed in a burst for the packet type. Range: 1 through 100,000 packets Default: 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 show ddos-protection protocols parameters brief command from operational mode.
Required Privilege Level	admin —To view this statement in the configuration. admin-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring DDoS Protection Policers for Individual Packet Types on page 10

burst-scale (DDoS)

Syntax	<code>burst-scale <i>percentage</i>;</code>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>) fpc <i>slot-number</i>]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	(MX Series routers with Trio MPCs only) Configure the percentage by which the DDoS burst limit is scaled down for the packet type on the specified card.
Options	<p><i>percentage</i>—Percentage multiplied by the burst limit to reduce the number of packets allowed in a burst for the packet type.</p> <p>Range: 1 through 100 percent</p> <p>Default: 100</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring DDoS Protection Policers for Individual Packet Types on page 10

bypass-aggregate (DDoS)

Syntax	<code>bypass-aggregate;</code>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group</i> <i>packet-type</i>]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	(MX Series routers with Trio MPCs only) Prevent this packet type from being considered by the DDoS aggregate policer. Traffic for the packet type is still included in traffic statistics.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring DDoS Protection Policers for Individual Packet Types on page 10

ddos-protection (DDoS)

Syntax	<pre> ddos-protection global { disable-fpc; disable-logging; disable-routing-engine; } protocols protocol-group (aggregate packet-type) { bandwidth packets-per-second; burst size; bypass-aggregate; disable-fpc; disable-logging; disable-routing-engine; fpc slot-number { bandwidth-scale percentage; burst-scale percentage; disable-fpc; } priority level; recover-time seconds; } 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; } </pre>
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	<p>(MX Series routers with Trio MPCs only) Configure DDoS policers.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Protection Against DDoS Attacks on page 9

disable-fpc (DDoS)

Syntax	disable-fpc;
Hierarchy Level	[edit system ddos-protection global], [edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)], [edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>) fpc <i>slot-number</i>]
Release Information	Statement introduced in Junos OS Release 11.2. 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 Trio MPCs only) 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. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Disabling DDoS Protection Policers and Logging Globally on page 10 • Configuring DDoS Protection Policers for Individual Packet Types on page 10

disable-logging (DDoS)

Syntax	disable-logging;
Hierarchy Level	[edit system ddos-protection global], [edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)]
Release Information	Statement introduced in Junos OS Release 11.2. 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 Trio MPCs only) Disable router-wide logging of DDoS violation events for debugging purposes for a particular packet type within a protocol group or globally for all packet types in all protocols.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Disabling DDoS Protection Policers and Logging Globally on page 10

disable-routing-engine (DDoS)

Syntax	disable-routing-engine;
Hierarchy Level	[edit system ddos-protection global], [edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)
Release Information	Statement introduced in Junos OS Release 11.2.
Description	(MX Series routers with Trio MPCs only) 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.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Disabling DDoS Protection Policers and Logging Globally on page 10

fpc (DDoS)

Syntax	fpc <i>slot-number</i> ; bandwidth-scale <i>percentage</i> ; burst-scale <i>percentage</i> ; disable-fpc ; }
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	(MX Series routers with Trio MPCs only) Modify the DDoS policer for the packet type on the specified card.
Options	<i>slot-number</i> —Slot number of the card. Range: Depends on the router model The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring DDoS Protection Policers for Individual Packet Types on page 10

global (DDoS)

Syntax	<pre>global { disable-fpc; disable-logging; disable-routing-engine; }</pre>
Hierarchy Level	[edit system ddos-protection]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	<p>(MX Series routers with Trio MPCs only) Modify DDoS policers and event logging globally for all protocols.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring DDoS Protection Policers for Individual Packet Types on page 10

priority (DDoS)

Syntax	<code>priority <i>level</i>;</code>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	<p>(MX Series routers with Trio MPCs only) 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.</p>
Options	<i>level</i> —Priority of the packet type, low, medium, or high.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring DDoS Protection Policers for Individual Packet Types on page 10

protocols (DDoS)

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

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

Release Information Statement introduced in Junos OS Release 11.2.

Description (MX Series routers with Trio MPCs only) 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**—DHCP OFFER packets.
- **release**—DHCP RENEW packets.
- **renew**—DHCP RENEW packets.
- **request**—DHCP REQUEST 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.
- **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.
- **ipv4-unclassified**—All unclassified host-bound IPv4 traffic.
- **ipv6-unclassified**—All unclassified host-bound IPv6 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.
 - **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.
- **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:

- **anccp**—ANCP traffic.
- **anccpv6**—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.
- **dhcpcv4**—DHCPv4 traffic.
- **dhcpcv6**—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.
- **ftp**—FTP traffic.
- **ftpv6**—FTPv6 traffic.
- **gre**—GRE traffic.
- **icmp**—ICMP traffic.
- **igmp**—IGMP traffic
- **igmp-snoop**—Control traffic for IGMP snooping.
- **igmpv4v6**—IGMP v4/v6 traffic.
- **igmpv6**—IGMPv6 traffic.
- **ip-fragments**—IP fragments traffic.
- **ip-options**—IP traffic with IP packet header options.
- **ipv4-unclassified**—Unclassified IPv4 host-bound traffic.

- **ipv6-unclassified**—Unclassified IPv6 host-bound traffic.
- **isis**—IS-IS traffic.
- **jfm**—JFM 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.
- **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.
- **virtual-chassis**—Virtual chassis traffic.
- **vrrp**—VRRP traffic.
- **vrrpv6**—VRRPv6 traffic.

The remaining statements are explained separately.

Required Privilege Level	admin—To view this statement in the configuration.
	admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring DDoS Protection Policers for Individual Packet Types on page 10

recover-time (DDoS)

Syntax	<code>recover-time <i>seconds</i>;</code>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group</i> (aggregate <i>packet-type</i>)]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	(MX Series routers with Trio MPCs only) 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.
Options	<i>seconds</i> —Period required for the traffic to recover. Range: 1 through 3600 seconds Default: 300
Required Privilege Level	admin —To view this statement in the configuration. admin-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring DDoS Protection Policers for Individual Packet Types on page 10

traceoptions (DDoS)

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; level (all error info notice verbose warning); no-remote-trace; }</pre>
Hierarchy Level	[edit system ddos-protection]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Define tracing operations for DDoS processes.
Options	<p>file <i>filename</i>—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 /var/log.</p> <p>files <i>number</i>—(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 size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none">• all—Trace all operations.• config—Trace configuration events.• events—Trace all events.• gres—Trace GRES events.• init—Trace daemon initialization.• memory—Trace memory management code.• protocol—Trace DDoS protocol processing events.• rt-sock—Trace routing socket events.• signal—Trace signal handling events.• state—Trace state machine events.• timer—Trace timer events.• ui—Trace user interface events. <p>level—Level of tracing to perform. You can specify any of the following levels:</p> <ul style="list-style-type: none">• all—Match all levels.

- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

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

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

Range: 10,240 through 1,073,741,824

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level	trace—To view this statement in the configuration.
	trace-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Tracing DDoS Protection Operations on page 13

PART 2

Indexes

- [Index on page 51](#)
- [Index of Statements and Commands on page 53](#)

Index

B

bandwidth statement	
DDoS protection.....	31
bandwidth-scale statement	
DDoS protection.....	32
burst statement	
DDoS protection.....	32
burst-scale statement	
DDoS protection.....	33
bypass-aggregate statement	
DDoS protection.....	33

D

DDoS protection	
configuration example.....	17
configuration overview.....	9
disabling policers and logging globally.....	10
flags for tracing operations.....	16
log file access for tracing operations.....	15
log file size and number.....	14
log filenames.....	14
logging	
disabling globally.....	10
message severity levels for tracing	
operations.....	16
overview.....	3
packet-level configuration.....	10
policers	
aggregate.....	4
disabling globally.....	10
disabling individual.....	10
hierarchy.....	5
packet-level configuration.....	10
protocol.....	4
scaling.....	5
regular expressions for tracing operations.....	15
tracing operations.....	13
traffic priority	
aggregate.....	4
verifying configuration.....	16

DDoS protection statements	
bandwidth.....	31
bandwidth-scale.....	32
burst.....	32
burst-scale.....	33
bypass-aggregate.....	33
ddos-protection.....	34
disable-fpc.....	35
disable-logging.....	35
disable-routing-engine.....	36
fpc.....	36
global.....	37
priority.....	37
protocols.....	38
recover-time.....	45
traceoptions.....	46
ddos-protection statement	
DDoS protection.....	34
denial-of-service attacks	
protecting against See DDoS Protection	
disable-fpc statement	
DDoS protection.....	35
disable-logging statement	
DDoS protection.....	35
disable-routing-engine statement	
DDoS protection.....	36
distributed denial of service See DDoS protection	
F	
fpc statement	
DDoS protection.....	36
G	
global statement	
DDoS protection.....	37
L	
log files	
filenames for DDoS protection.....	14
number of DDoS protection.....	14
size of DDoS protection.....	14
P	
priority statement	
DDoS protection.....	37
protocols statement	
DDoS protection.....	38

R

recover-time statement	
DDoS protection.....	45

T

traceoptions statement	
DDoS protection.....	46
tracing operations	
DDoS protection.....	13

Index of Statements and Commands

B

bandwidth statement	
DDoS protection.....	31
bandwidth-scale statement	
DDoS protection.....	32
burst statement	
DDoS protection.....	32
burst-scale statement	
DDoS protection.....	33
bypass-aggregate statement	
DDoS protection.....	33

D

DDoS protection statements	
bandwidth.....	31
bandwidth-scale.....	32
burst.....	32
burst-scale.....	33
bypass-aggregate.....	33
ddos-protection.....	34
disable-fpc.....	35
disable-logging.....	35
disable-routing-engine.....	36
fpc.....	36
global.....	37
priority.....	37
protocols.....	38
recover-time.....	45
traceoptions.....	46
ddos-protection statement	
DDoS protection.....	34
disable-fpc statement	
DDoS protection.....	35
disable-logging statement	
DDoS protection.....	35
disable-routing-engine statement	
DDoS protection.....	36

F

fpc statement	
DDoS protection.....	36

G

global statement	
DDoS protection.....	37

P

priority statement	
DDoS protection.....	37
protocols statement	
DDoS protection.....	38

R

recover-time statement	
DDoS protection.....	45

T

traceoptions statement	
DDoS protection.....	46

