JUNIPER NETWORKS

Distributed Denial-of-Service Protection

Published: 2012-12-04

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

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

List of Figures

List of Tables

About the Documentation

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

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.xsl;
       }
     }
   }
   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.xsl; }
   ```

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 xi 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 xi 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
Italic text like this	• Introduces or emphasizes important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	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** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• 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** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web 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

CHAPTER 1

Distributed DDoS Protection in Subscriber Access Networks

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 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 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

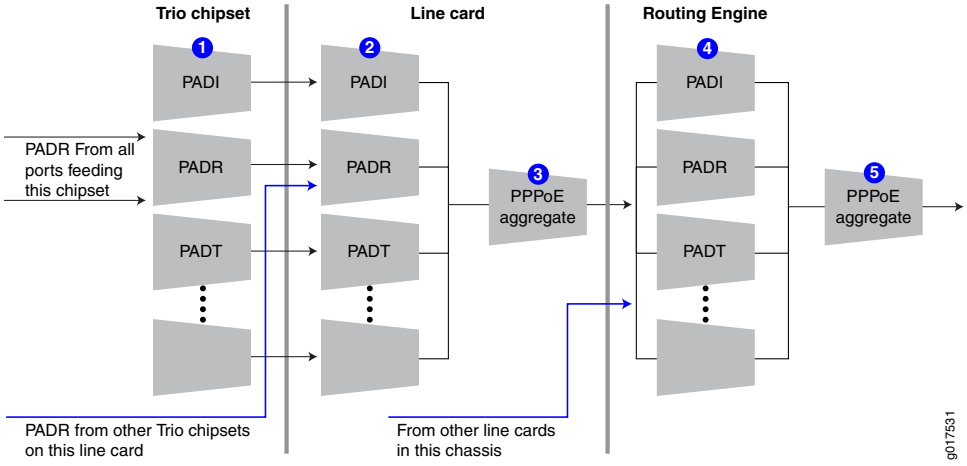
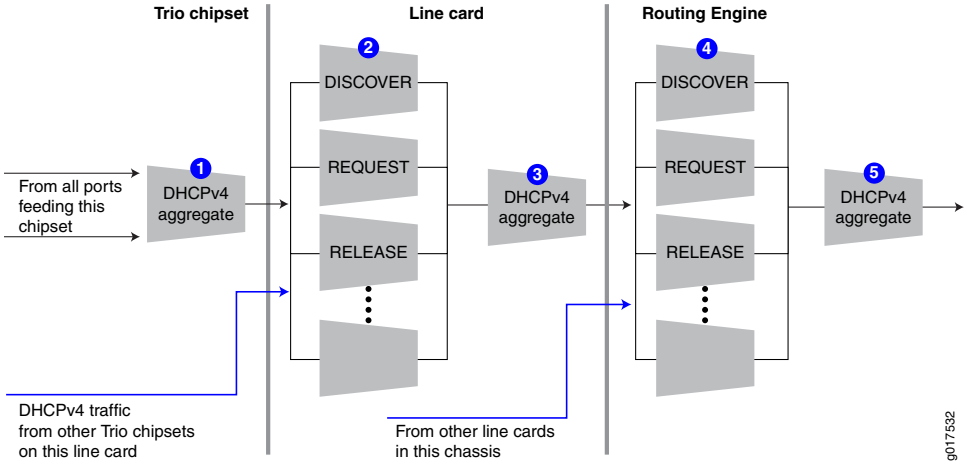


Figure 2: Policer Hierarchy for DHCPv4 Packets



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 11
- DDoS Protection Flow Detection Overview

PART 2

Configuration

CHAPTER 2

Configuration Overview

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 17.

2. (Optional) Configure DDoS settings for individual packet types.

   See "Configuring DDoS Protection Policers for Individual Packet Types" on page 13.

3. (Optional) Configure tracing for DDoS operations.

   See "Tracing DDoS Protection Operations" on page 93.

Related Documentation

- Distributed Denial-of-Service (DDoS) Protection Overview on page 3
- Example: Configuring DDoS Protection on page 19

CHAPTER 3

Configuration Tasks for Distributed DDoS

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 11

- For a list of supported protocol groups and packet types, see protocols on page 38.
- Example: Configuring DDoS Protection on page 19

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 11

CHAPTER 4

Example

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

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 22
- Verifying the PPPoE DDoS Configuration on page 25

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 1received 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 1received 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 + 4,094030)] 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 11

CHAPTER 5

Configuration Statements

[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;
        }
        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 11
- Configuring Flow Detection for DDoS Protection

bandwidth (DDoS)

Syntax bandwidth *packets-per-second*;

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

Release Information Statement introduced in Junos OS Release 11.2.

Description (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.

Options *packets-per-second*—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

- Configuring DDoS Protection Policers for Individual Packet Types on page 13

bandwidth-scale (DDoS)

Syntax bandwidth-scale *percentage*;

Hierarchy Level [edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*) fpc *slot-number*]

Release Information Statement introduced in Junos OS Release 11.2.

Description (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.

Options *percentage*—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 burst *size*;

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

Release Information Statement introduced in Junos OS Release 11.2.

Description (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.

Options *size*—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

- Configuring DDoS Protection Policers for Individual Packet Types on page 13

burst-scale (DDoS)

Syntax burst-scale *percentage*;

Hierarchy Level [edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*) fpc *slot-number*]

Release Information Statement introduced in Junos OS Release 11.2.

Description (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.

Options *percentage*—Percentage multiplied by the burst limit to reduce the number of packets allowed in a burst 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.

Related Documentation
- Configuring DDoS Protection Policers for Individual Packet Types on page 13

bypass-aggregate (DDoS)

Syntax bypass-aggregate;

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

Release Information Statement introduced in Junos OS Release 11.2.

Description (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.

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

Related Documentation
- Configuring DDoS Protection Policers for Individual Packet Types on page 13

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;
  }
  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.

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 Protection Against DDoS Attacks on page 11
- Configuring Flow Detection for DDoS Protection

disable-fpc (DDoS)

Syntax disable-fpc;

Hierarchy Level [edit system ddos-protection global],
[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)],
[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*) fpc *slot-number*]

Release Information Statement introduced in Junos OS Release 11.2.
Support at the **[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]** 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.
admin-control—To add this statement to the configuration.

Related Documentation
- Disabling DDoS Protection Policers and Logging Globally on page 17
- Configuring DDoS Protection Policers for Individual Packet Types on page 13

disable-logging (DDoS)

Syntax disable-logging;

Hierarchy Level [edit system ddos-protection global],
[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]

Release Information Statement introduced in Junos OS Release 11.2.
Support at the **[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]** hierarchy level introduced in Junos OS Release 12.1.

Description (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.

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

Related Documentation

- Disabling DDoS Protection Policers and Logging Globally on page 17
- Configuring DDoS Protection Policers for Individual Packet Types on page 13
- Disabling Automatic Logging of Culprit Flow Events for a Packet Type

disable-routing-engine (DDoS)

Syntax disable-routing-engine;

Hierarchy Level [edit system ddos-protection global],
[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)

Release Information Statement introduced in Junos OS Release 11.2.

Description (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.

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

Related Documentation

- Disabling DDoS Protection Policers and Logging Globally on page 17

fpc (DDoS)

Syntax

```
fpc slot-number;
  bandwidth-scale percentage;
  burst-scale percentage;
  disable-fpc;
}
```

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

Release Information Statement introduced in Junos OS Release 11.2.

Description (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.

Options ***slot-number***—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

- Configuring DDoS Protection Policers for Individual Packet Types on page 13

global (DDoS)

Syntax

```
global {
  disable-fpc;
  disable-logging;
  disable-routing-engine;
  flow-detection;
  flow-report-rate;
  violation-report-rate;
}
```

Hierarchy Level [edit system ddos-protection]

Release Information Statement introduced in Junos OS Release 11.2.

Description Modify DDoS policers, event logging, and flow detection globally for all protocols.

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

- Disabling DDoS Protection Policers and Logging Globally on page 17

priority (DDoS)

Syntax priority *level*;

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

Release Information Statement introduced in Junos OS Release 11.2.

Description (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.

Options ***level***—Priority of the packet type, low, medium, or high.

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

Related Documentation

- Configuring DDoS Protection Policers for Individual Packet Types on page 13

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;
}
```

Hierarchy Level [edit system ddos-protection]

Release Information Statement introduced in Junos OS Release 11.2.

Description (MX Series routers with only MPCs or T4000 Core Routers with only FPC5s) 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**—DHCPLEASEQUERYpackets.
- **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.
- **ipv4-unclassified**—All unclassified host-bound IPv4 traffic.
- **ipv6-unclassified**—All unclassified host-bound IPv6 traffic.

- **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.
- **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.
- **ipv4-unclassified**—Unclassified IPv4 host-bound traffic.
- **ipv6-unclassified**—Unclassified IPv6 host-bound traffic.
- **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.
- **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

- Configuring DDoS Protection Policers for Individual Packet Types on page 13

recover-time (DDoS)

Syntax recover-time *seconds*;

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

Release Information Statement introduced in Junos OS Release 11.2.

Description (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.

Options ***seconds***—Period required for the traffic to recover.

Range: 1 through 3600 seconds

Default: 300

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

Related Documentation

- Configuring DDoS Protection Policers for Individual Packet Types on page 13

traceoptions (DDoS)

Syntax

```
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 ddos-protection]

Release Information Statement introduced in Junos OS Release 11.2.

Description Define tracing operations for DDoS protection processes.

Options

file *filename*—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**.

files *number*—(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.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **config**—Trace configuration events.
- **events**—Trace all events.
- **gres**—Trace GRES events.
- **init**—Trace daemon initialization.
- **ipc**—Trace IPC events.
- **memory**—Trace memory management code.
- **protocol**—Trace DDoS protocol processing events.
- **rtsock**—Trace routing socket events.
- **signal**—Trace signal handling events.
- **socket**—Trace socket events.
- **state**—Trace state machine events.
- **timer**—Trace timer events.
- **ui**—Trace user interface events.

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

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

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

no-remote-trace—Disable remote tracing.

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

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

Syntax: ***size*****k** to specify KB, ***size*****m** to specify MB, or ***size*****g** 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
- Tracing DDoS Protection Operations on page 93

violation (DDoS)

Syntax

```
violation {
  disable-logging;
}
```

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

Release Information Statement introduced in Junos OS Release 11.2.

Description (MX Series routers with Trio MPCs only) Disable event logging when a DDoS violation occurs; that is, when the configured policer value is exceeded.

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

Related Documentation
- Configuring DDoS Protection Policers for Individual Packet Types on page 13

PART 3

Administration

CHAPTER 6

Verifying and Monitoring Configurations

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
- Junos OS Operational Mode Commands

CHAPTER 7

Monitoring Commands

clear ddos-protection protocols

Syntax **clear ddos-protection protocols**
<*protocol-group* <*packet-type*>> (culprit-flows | states | statistics)

Release Information Command introduced in Junos OS Release 11.2.
Option **culprit-flows** 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 ***protocol-group***—(Optional) Protocol group that is cleared. See show ddos-protection protocols for a list of available groups.

packet-type—(Optional) Packet type in a particular protocol group that is cleared. See show ddos-protection protocols for a list of available packet types.

culprit-flows—Clear culprit flows for a packet type, for a protocol group, or for all protocol groups.

states—Clear DDoS protection violation states for a packet type, for a protocol group, or for all protocol groups.

statistics—Clear DDoS protection statistics such as packet counts and rates for a packet type, for a protocol group, or for all protocol groups.

Required Privilege Level clear

Related Documentation
- show ddos-protection protocols on page 55
- show ddos-protection statistics on page 89
- show ddos-protection version on page 90

List of Sample Output clear ddos-protection protocols on page 54

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ddos-protection protocols

```
user@host> clear ddos-protection protocols dhcpv4 bootp states
```

show ddos-protection protocols

Syntax **show ddos-protection protocols <*protocol-group* (aggregate | *packet-type*)>**

Release Information Command introduced in Junos OS Release 11.2.

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

Options **none**—Display information for all packet types in all protocol groups.

aggregate—(Optional) Display DDoS protection information for the aggregate policer. The **aggregate** option is available for all protocol groups.

packet-type—(Optional) Display DDoS protection information for the specified packet type in the protocol group. The available packet types vary by protocol group. Only an aggregate policer is available for protocol groups that are not in the following list:

- **dhcpv4**—The following packet types are available for DHCPv4 traffic:
  - **ack**—DHCPACK packets.
  - **bad-packets**—DHCPv4 packets with bad formats.
  - **bootp**—DHCPBOOTP packets.
  - **decline**—DHCPDECLINE packets.
  - **discover**—DHCDISCOVER packets.
  - **force-renew**—DHCPFORCERENEW packets.
  - **inform**—DHCPINFORM packets.
  - **lease-active**—DHCPLEASEACTIVE packets.
  - **lease-query**—DHCPLEASEQUERYpackets.
  - **lease-unassigned**—DHCPLEASEUNASSIGNED packets.
  - **lease-unknown**—DHCPLEASEUNKNOWN packets.
  - **nak**—DHCPNAK packets.
  - **no-message-type**—DHCP packets that are missing the message type..
  - **offer**—DHCOFFER packets.
  - **release**—DHCPACK packets.
  - **renew**—DHCPRENEW packets.

- **request**—DHCPREQUEST packets.
- **unclassified**— All unclassified packets in the protocol group.

- **dhcpv6**—The following packet types are available for DHCPv6 traffic:
  - **advertise**—ADVERTISE packets.
  - **confirm**—CONFIRM packets.
  - **decline**—DECLINE packets.
  - **information-request**—INFORMATION-REQUEST packets.
  - **leasequery**—LEASEQUERY packets.
  - **leasequery-data**—LEASEQUERY-DATA packets.
  - **leasequery-done**—LEASEQUERY-DONE packets.
  - **leasequery-reply**—LEASEQUERY-REPLY packets.
  - **rebind**—REBIND packets.
  - **reconfigure**—RECONFIGURE packets.
  - **relay-forward**—RELAY-FORWARD packets.
  - **relay-reply**—RELAY-REPLY packets.
  - **release**—RELEASE packets.
  - **renew**—RENEW packets.
  - **reply**—REPLY packets.
  - **request**—REQUEST packets.
  - **solicit**—SOLICIT packets.
  - **unclassified**— All unclassified packets in the protocol group.
- **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.

- **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.
- **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.
- **ipv4-unclassified**—All unclassified IPv4 host-bound traffic.
- **ipv6-unclassified**—All unclassified IPv6 host-bound traffic.
- **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.
- **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.
- **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.

Required Privilege Level view

Related Documentation

- clear ddos-protection protocols on page 54
- show ddos-protection protocols culprit-flows
- show ddos-protection protocols flow-detection
- show ddos-protection protocols parameters on page 70
- show ddos-protection protocols statistics on page 77
- show ddos-protection protocols violations on page 87

List of Sample Output

show ddos-protection protocols on page 65
show ddos-protection protocols (Specific Packet Type with Flow Detection Disabled) on page 67
show ddos-protection protocols (Specific Packet Type with Flow Detection Enabled and Automatic) on page 68
show ddos-protection protocols (Specific Packet Type with Bandwidth Violation) on page 68

Output Fields Table 3 on page 61 lists the output fields for the **show ddos-protection protocols** command. Output fields are listed in the approximate order in which they appear.

Table 3: show ddos-protection protocols Output Fields

Field Name	Field Description
Packet types	Number of packet types
Modified	Number of packets for which policer values have been modified from the default.
Received traffic	Number of traffic flows received.
Currently violated	Number of flows that are currently violating the flow bandwidth limit.

Table 3: show ddos-protection protocols Output Fields *(continued)*

Field Name	Field Description
Currently tracked flows	Number of active flows that are being tracked as culprit flows by flow detection.
Total detected flows	Total number of culprit flows that have been detected, including those that have recovered or timed out.
Protocol Group	Name of protocol group.
Packet type	Name of packet type in protocol group.
Bandwidth	Bandwidth policer value; number of packets per second that is allowed before a violation is declared.
Burst	Burst policer value; the maximum number of packets that is allowed in a burst before a violation is declared.
Priority	Priority of the packet type for individual packet policers that enables more important traffic to pass through in the event of traffic congestion: **low**, **medium**, or **high**. Lower priority packets can be dropped when insufficient bandwidth is available.
Recover time	Time that must pass since the last violation before the traffic flow is considered to have recovered from the attack. A notification is generated when the timer expires.
Enabled	State of the policer, enabled (**Yes**), disabled (**No**), or partially disabled (**Partial**); **Partial** indicates that only some of the policer instances are disabled for the policer.
Bypass aggregate	State of the bypass aggregate configuration: • Yes—The aggregate policer is bypassed. • No—The aggregate policer is enforced. This field appears only for individual policers.

Table 3: show ddos-protection protocols Output Fields *(continued)*

Field Name	Field Description
Flow detection configuration	State of flow detection configured on the router: • Detection mode—Mode of operation for suspicious flow detection: automatic, off, or on. • Log flows—State of automatic logging of suspicious traffic flows: on (**Yes**) or off (**No**). • Timeout flows—State of culprit flow timeout behavior: flow is suppressed for a configured timeout period (**Yes**) or flow is suppressed until it is no longer in violation (**No**). • 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. • 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. • Timeout time—Time in seconds that a culprit flow is suppressed, if timeouts have been enabled. • 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. ◦ Detection mode—State of flow detection: automatic, off, or on. Control mode—Mode of controlling culprit traffic: dropped, kept, or policed back to within the allowed bandwidth. Flow rate—Bandwidth allowed for the control traffic in packets per second.
System-wide information	The following information collected for the router: • A message indicates whether the policer has been violated. • No. of FPCs currently receiving excess traffic—Number of cards that are currently in violation of a policer. • No. of FPCs that have received excess traffic—Number of cards that have at some point been in violation of a policer. • Violation first detected at—Timestamp of the first violation. • Violation last seen at—Timestamp of the last observed violation. • Duration of violation—Length of the violation. • Number of violations—Number of times the violation has occurred. • Received—Number of packets received at all card slots and the Routing Engine. • Dropped—Number of packets dropped regardless of where they were dropped. • Arrival rate—Current traffic rate for packets arriving from all cards and at the Routing Engine. • Max arrival rate—Highest traffic rate for packets arriving from all cards and at the Routing Engine.

Table 3: show ddos-protection protocols Output Fields *(continued)*

Field Name	Field Description
Routing Engine information	The following information collected for the Routing Engine: • Bandwidth—Maximum number of packets per second that is allowed. • Burst—Maximum number of packets that is allowed in a burst. • A message indicates the State of the policer, enabled (**Yes**) or disabled (**No**). • 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. • Violation first detected at—Timestamp of the first violation. • Violation last seen at—Timestamp of the last observed violation. • Duration of violation—Length of the violation. • Number of violations—Number of times the violation has occurred. • Received—Number of packets received at the Routing Engine from all cards. • Dropped—Number of packets dropped at the Routing Engine; includes packets dropped by the aggregate policer and by individual protocol policers. • Arrival rate—Current traffic rate for packets arriving at the Routing Engine from all cards. • Max arrival rate—Highest traffic rate for packets arriving at the Routing Engine from all cards. • Dropped by aggregate policer—Number of packets dropped by the aggregate policer. • Dropped by individual policers—Number of packets dropped by individual policer.
FPC slot information	The following information collected for the card in the indicated slot: • Bandwidth—Bandwidth scaling percentage and the number of packets per second that is allowed before a violation is declared. • Burst—Burst scaling percentage and the maximum number of packets that is allowed in a burst before a violation is declared. • A message indicates whether the policer has been violated. • Violation first detected at—Timestamp of the first violation. • Violation last seen at—Timestamp of the last observed violation. • Duration of violation—Length of the violation. • Number of violations—Number of times the violation has occurred. • Received—Number of packets received on the line card. • Dropped—Number of packets dropped at the line card; includes packets dropped by the aggregate policer and by individual protocol policers. • Arrival rate—Current traffic rate for packets arriving at the line card. • Max arrival rate—Highest traffic rate for packets arriving at the line card. • Dropped by this policer—Number of packets dropped by the individual policer. • Dropped by aggregate policer—Number of packets dropped by the aggregate policer.

Table 3: show ddos-protection protocols Output Fields *(continued)*

Field Name	Field Description
Bypass aggr.	State of the bypass aggregate configuration: • Yes—The aggregate policer configuration is bypassed. • No—The aggregate policer configuration is enforced. Dashes indicate that the bypass aggregate configuration is not available; this is possible only for aggregate policers.
FPC Mod	Indicates whether configuration has changed from the default for any line cards. • No—The default configuration has not changed from the default for the packet type. • Yes—The default configuration has changed from the default for the packet type
Op mode	Mode of operation for suspicious flow detection for the packet type: always-on (**on**), (**auto**), or disabled (**off**).
Policer BW (pps)	Bandwidth policer value; number of packets per second that is allowed before a violation is declared.
Aggr level Op:Fc:Bwidth (pps)	Flow operation mode, flow control mode, and flow bandwidth for traffic of the packet type at each traffic flow aggregation level: subscriber (**sub**), logical interface (**ifl**), and physical interface (**ifd**).
Log flow	State of automatic logging of suspicious traffic flows for the packet type: on (**Yes**) or off (**No**).
Time out	State of culprit flow timeout behavior for the packet type: flow is suppressed or monitored for a configured timeout period (**Yes**) or flow is suppressed or monitored until it is no longer in violation (**No**).

Sample Output

show ddos-protection protocols

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

Packet types: 190, Modified: 0, Received traffic: 12, Currently violated: 3
Currently tracked flows: 0, Total detected flows: 0
* = User configured value

Protocol Group: IPv4-Unclassified

  Packet type: aggregate (Aggregate for unclassified host-bound IPv4 traff)
    Aggregate policer configuration:
      Bandwidth:        2000 pps
      Burst:            10000 packets
      Recover time:     300 seconds
      Enabled:          Yes
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
```

```
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          2000 pps
    System-wide information:
      Aggregate bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Bandwidth: 2000 pps, Burst: 10000 packets, enabled
      Aggregate policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by individual policers: 0
    FPC slot 1 information:
      Bandwidth: 100% (2000 pps), Burst: 100% (10000 packets), enabled
      Aggregate policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by individual policers: 0
        Dropped by flow suppression:    0

…

Protocol Group: PPPoE

  Packet type: aggregate (Aggregate for all PPPoE control traffic)
    Aggregate policer configuration:
      Bandwidth:        2000 pps
      Burst:            2000 packets
      Recover time:     300 seconds
      Enabled:          Yes
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          2000 pps
    System-wide information:
      Aggregate bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Bandwidth: 2000 pps, Burst: 2000 packets, enabled
      Aggregate policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by individual policers: 0
    FPC slot 1 information:
      Bandwidth: 100% (2000 pps), Burst: 100% (2000 packets), enabled
      Aggregate policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by individual policers: 0
        Dropped by flow suppression:    0

  Packet type: padi (PPPoE PADI)
```



```
    Individual policer configuration:
      Bandwidth:        500 pps
      Burst:            500 packets
      Priority:         Low
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          500 pps
    System-wide information:
      Bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Bandwidth: 500 pps, Burst: 500 packets, enabled
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
        Dropped by flow suppression:  0
...
```

show ddos-protection protocols (Specific Packet Type with Flow Detection Disabled)

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

Protocol Group: PPPoE

  Packet type: padi (PPPoE PADI)
    Individual policer configuration:
      Bandwidth:        500 pps
      Burst:            500 packets
      Priority:         Low
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    Flow detection configuration:
      Detection mode: Off*       Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          500 pps
    System-wide information:
      Bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
```

```
    Dropped:   0                    Max arrival rate: 0 pps
  Routing Engine information:
    Bandwidth: 500 pps, Burst: 500 packets, enabled
    Policer is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
    Policer is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
      Dropped by flow suppression:  0
```

show ddos-protection protocols (Specific Packet Type with Flow Detection Enabled and Automatic)

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

Protocol Group: PPPoE

  Packet type: padi (PPPoE PADI)
    Individual policer configuration:
      Bandwidth:        500 pps
      Burst:            500 packets
      Priority:         Low
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          500 pps
    System-wide information:
      Bandwidth is never violated
      Received:  0                    Arrival rate:     0 pps
      Dropped:   0                    Max arrival rate: 0 pps
    Routing Engine information:
      Bandwidth: 500 pps, Burst: 500 packets, enabled
      Policer is never violated
      Received:  0                    Arrival rate:     0 pps
      Dropped:   0                    Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
      Policer is never violated
      Received:  0                    Arrival rate:     0 pps
      Dropped:   0                    Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
        Dropped by flow suppression:  0
```

show ddos-protection protocols (Specific Packet Type with Bandwidth Violation)

```
user@host> show ddos-protection protocols bfd
Packet types: 1, Modified: 0, Received traffic: 1, Currently violated: 1
Currently tracked flows: 1, Total detected flows: 1
* = User configured value
```

```
Protocol Group: BFD

  Packet type: aggregate (Aggregate for all bfd traffic)
    Aggregate policer configuration:
      Bandwidth:        20000 pps
      Burst:            20000 packets
      Recover time:     300 seconds
      Enabled:          Yes
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          20000 pps
    System-wide information:
      Aggregate bandwidth is being violated!
        No. of FPCs currently receiving excess traffic: 1
        No. of FPCs that have received excess traffic:  1
        Violation first detected at: 2012-10-24 23:40:20 EDT
        Violation last seen at:      2012-10-25 10:25:48 EDT
        Duration of violation: 10:45:28 Number of violations: 1
      Received:  1173471731          Arrival rate:     30304 pps
      Dropped:   399135607           Max arrival rate: 30331 pps
      Flow counts:
        Aggregation level     Current       Total detected
        Subscriber            1             1
        Total                 1             1
    Routing Engine information:
      Bandwidth: 20000 pps, Burst: 20000 packets, enabled
      Aggregate policer is never violated
      Received:  366831604           Arrival rate:     0 pps
      Dropped:   0                   Max arrival rate: 9522 pps
        Dropped by individual policers: 0
    FPC slot 1 information:
      Bandwidth: 100% (20000 pps), Burst: 100% (20000 packets), enabled
      Aggregate policer is currently being violated!
        Violation first detected at: 2012-10-24 23:40:21 EDT
        Violation last seen at:      2012-10-25 10:25:48 EDT
        Duration of violation: 10:45:27 Number of violations: 1
      Received:  1173471731          Arrival rate:     30304 pps
      Dropped:   399135607           Max arrival rate: 30331 pps
        Dropped by individual policers: 0
        Dropped by aggregate policer:   398854530
        Dropped by flow suppression:    281077
      Flow counts:
        Aggregation level     Current       Total detected   State
        Subscriber            1             1                Active
        Logical-interface     0             0                Active
        Physical-interface    0             0                Active
        Total                 1             1
```

show ddos-protection protocols parameters

Syntax **show ddos-protection protocols <*protocol-group*> parameters <brief | detail | terse>**

Release Information Command introduced in Junos OS Release 11.2.

Description Display DDoS protection configuration information for all protocol groups or for a particular protocol group.

Options **none**—Display information for all protocol groups.

brief | detail | terse—(Optional) Display the specified level of output.

- **brief**—Display basic function information.
- **detail**—Add information to the **brief** output; it is identical to the output displayed when you choose no option. The **brief** and **detail** options display information for all protocol groups, which can be a long list.
- **terse**—Display the same level of information as the **brief** option but only for active protocol groups—groups that show traffic in the **Received (packets)** column.

protocol-group—(Optional) Display information for a particular protocol group. See show ddos-protection protocols for a list of available groups.

Required Privilege Level view

Related Documentation

- clear ddos-protection protocols on page 54
- show ddos-protection protocols on page 55
- show ddos-protection protocols culprit-flows
- show ddos-protection protocols flow-detection
- show ddos-protection protocols statistics on page 77
- show ddos-protection protocols violations on page 87

List of Sample Output

show ddos-protection protocols parameters on page 72
show ddos-protection protocols parameters brief on page 73
show ddos-protection protocols dhcpv4 parameters brief on page 74
show ddos-protection protocols dhcpv4 parameters terse on page 75
show ddos-protection protocols dhcpv4 parameters on page 75

Output Fields Table 4 on page 71 lists the output fields for the **show ddos-protection protocols parameters** command. Output fields are listed in the approximate order in which they appear.

Table 4: show ddos-protection protocols parameters Output Fields

Field Name	Field Description	Level of Output
Protocol Group	Name of protocol group.	All levels
Packet type	Name of packet type in protocol group.	All levels
Bandwidth	Bandwidth policer value; number of packets per second that is allowed before a violation is declared. In the **brief** output, an asterisk indicates the value has been modified from the default.	All levels
Burst	Burst policer value; the maximum number of packets that is allowed in a burst before a violation is declared. In the **brief** output, an asterisk indicates the value has been modified from the default.	All levels
Priority	Priority of the packet type in the event of traffic congestion: **low**, **medium**, or **high**. Lower priority packets can be dropped when insufficient bandwidth is available. In the **brief** output, an asterisk indicates the value has been modified from the default.	All levels
Recover time	Time that must pass since the last violation before the traffic flow is considered to have recovered from the attack. A notification is generated when the timer expires. In the **brief** output, an asterisk indicates the value has been modified from the default.	All levels
Enabled	State of the policer, enabled (**Yes**) or disabled (**No**).	**detail** none
Bypass aggregate	State of the bypass aggregate configuration: • Yes—The aggregate policer is bypassed. • No—The aggregate policer is enforced. This field appears only for individual policers.	**detail** none
FPC slot information	The following configuration information for the card in the indicated slot: • Bandwidth—Bandwidth scale and the number of packets per second that is allowed before a violation is declared • Burst—Burst scale and the maximum number of packets that is allowed in a burst before a violation is declared • **enabled** or **disabled**—State of the line card policer	**detail** none
Number of policers modified	Number of policers that have been changed from the default configuration. An asterisk by a particular value indicates that value has been modified.	**brief terse**
Policer Enabled	State of the policer, enabled (**Yes**), disabled (**No**), or partially disabled (**part.**); **part.** indicates that only some of the policer instances are disabled for the policer.	**brief terse**

Table 4: show ddos-protection protocols parameters Output Fields *(continued)*

Field Name	Field Description	Level of Output
Bypass aggr.	State of the bypass aggregate configuration: • Yes—The aggregate policer is bypassed. • No—The aggregate policer is enforced. Dashes indicate that the bypass aggregate configuration is not available; this is possible only for aggregate policers.	**brief terse**
FPC Mod	Indicates whether configuration has changed from the default for any line cards. • No—The default configuration has not changed from the default for the packet type. • Yes—The default configuration has changed from the default for the packet type	**brief terse**

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    Packet      Bandwidth Burst  Priority Recover   Policer Bypass FPC
group       type        (pps)     (pkts)         time(sec) enabled aggr.  mod
ipv4-uncls  aggregate   20000     20000  medium   300       yes     --     no
ipv6-uncls  aggregate   20000     20000  medium   300       yes     --     no
dynvlan     aggregate   1000      500    low      300       yes     --     no
ppp         aggregate   16000     16000  medium   300       yes     --     no
ppp         unclass     1000      500    low      300       yes     no     no
ppp         lcp         12000     12000  low      300       yes     no     no
ppp         auth        2000      2000   medium   300       yes     no     no
ppp         ipcp        2000      2000   high     300       yes     no     no
ppp         ipv6cp      2000      2000   high     300       yes     no     no
ppp         mplscp      2000      2000   high     300       yes     no     no
ppp         isis        2000      2000   high     300       yes     no     no
pppoe       aggregate   800*      2000   medium   300       part.*  --     no
pppoe       padi        500       500    low      300       part.   no     no
pppoe       pado        0         0      low      300       part.   no     no
pppoe       padr        500       500    medium   300       part.   no     no
pppoe       pads        0         0      low      300       part.   no     no
pppoe       padt        1000      1000   high     300       part.   no     no
pppoe       padm        0         0      low      300       part.   no     no
pppoe       padn        0         0      low      300       part.   no     no
dhcpv4      aggregate   669*      5000   medium   300       yes     --     no
dhcpv4      unclass..   300       150    low      300       yes     no     no
dhcpv4      discover    100*      500    low      300       yes     no     no
dhcpv4      offer       1000      1000   low      300       yes     no     no
```

```
dhcpv4      request     1000      1000    medium   300       yes     no     no
dhcpv4      decline     500       500     low      300       yes     no     no
dhcpv4      ack         500       500     medium   300       yes     no     no
dhcpv4      nak         500       500     low      300       yes     no     no
dhcpv4      release     2000      2000    high     300       yes     no     no
dhcpv4      inform      500       500     low      300       yes     no     no
dhcpv4      renew       2000      2000    high     300       yes     no     no
dhcpv4      forcerenew  2000      2000    high     300       yes     no     no
dhcpv4      leasequery  2000      2000    high     300       yes     no     no
dhcpv4      leaseuna..  2000      2000    high     300       yes     no     no
dhcpv4      leaseunk..  2000      2000    high     300       yes     no     no
dhcpv4      leaseact..  2000      2000    high     300       yes     no     no
dhcpv4      bootp       300       300     low      300       yes     no     no
dhcpv4      no-msgtype  0         0       low      300       yes     no     no
dhcpv4      bad-pack..  0         0       low      300       yes     no     no

...

icmp        aggregate   20000     20000   high     300       yes     --     no
igmp        aggregate   20000     20000   high     300       yes     --     no
ospf        aggregate   20000     20000   high     300       yes     --     no
rsvp        aggregate   20000     20000   high     300       yes     --     no
pim         aggregate   20000     20000   high     300       yes     --     no
rip         aggregate   20000     20000   high     300       yes     --     no
ptp         aggregate   20000     20000   high     300       yes     --     no
bfd         aggregate   20000     20000   high     300       yes     --     no
lmp         aggregate   20000     20000   high     300       yes     --     no
ldp         aggregate   20000     20000   high     300       yes     --     no
msdp        aggregate   20000     20000   high     300       yes     --     no
bgp         aggregate   20000     20000   low      300       yes     --     no
vrrp        aggregate   20000     20000   high     300       yes     --     no
telnet      aggregate   20000     20000   low      300       yes     --     no
ftp         aggregate   20000     20000   low      300       yes     --     no
ssh         aggregate   20000     20000   low      300       yes     --     no
snmp        aggregate   20000     20000   low      300       yes     --     no
ancp        aggregate   20000     20000   low      300       yes     --     no

...
```

show ddos-protection protocols dhcpv4 parameters brief

```
user@host> show ddos-protection protocols dhcpv4 parameters brief
Number of policers modified: 2
Protocol    Packet      Bandwidth Burst  Priority Recover   Policer Bypass FPC
group       type        (pps)     (pkts)         time(sec) enabled aggr.  mod
dhcpv4      aggregate   669*      5000   medium   300       yes     --     no
dhcpv4      unclass..   300       150    low      300       yes     no     no
dhcpv4      discover    100*      500    low      300       yes     no     no
dhcpv4      offer       1000      1000   low      300       yes     no     no
dhcpv4      request     1000      1000   medium   300       yes     no     no
dhcpv4      decline     500       500    low      300       yes     no     no
dhcpv4      ack         500       500    medium   300       yes     no     no
dhcpv4      nak         500       500    low      300       yes     no     no
dhcpv4      release     2000      2000   high     300       yes     no     no
dhcpv4      inform      500       500    low      300       yes     no     no
dhcpv4      renew       2000      2000   high     300       yes     no     no
dhcpv4      forcerenew  2000      2000   high     300       yes     no     no
dhcpv4      leasequery  2000      2000   high     300       yes     no     no
dhcpv4      leaseuna..  2000      2000   high     300       yes     no     no
dhcpv4      leaseunk..  2000      2000   high     300       yes     no     no
dhcpv4      leaseact..  2000      2000   high     300       yes     no     no
dhcpv4      bootp       300       300    low      300       yes     no     no
```

```
dhcpv4      no-msgtype  0         0      low      300       yes     no      no
dhcpv4      bad-pack..  0         0      low      300       yes     no      no
```

show ddos-protection protocols dhcpv4 parameters terse

```
user@host> show ddos-protection protocols dhcpv4 parameters terse
Number of policers modified: 2
Protocol    Packet      Bandwidth Burst  Priority Recover   Policer Bypass FPC
group       type        (pps)     (pkts)         time(sec) enabled aggr.  mod
dhcpv4      aggregate   669*      5000   medium   300       yes     --     no
dhcpv4      discover    100*      500    low      300       yes     no     no
```

show ddos-protection protocols dhcpv4 parameters

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

  Packet type: aggregate (aggregate for all DHCPv4 traffic)
    Aggregate policer configuration:
      Bandwidth:        669 pps
      Burst:            5000 packets
      Priority:         medium
      Recover time:     300 seconds
      Enabled:          Yes
    FPC slot 1 information:
      Bandwidth: 100% (669 pps), Burst: 100% (5000 packets), enabled

  Packet type: unclassified (Unclassified DHCPv4 traffic)
    Individual policer configuration:
      Bandwidth:        300 pps
      Burst:            150 packets
      Priority:         low
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    FPC slot 1 information:
      Bandwidth: 100% (300 pps), Burst: 100% (150 packets), enabled

  Packet type: discover (DHCPv4 DHCPDISCOVER)
    Individual policer configuration:
      Bandwidth:        100 pps
      Burst:            500 packets
      Priority:         low
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    FPC slot 1 information:
      Bandwidth: 100% (100 pps), Burst: 100% (500 packets), enabled

  Packet type: offer (DHCPv4 DHCPOFFER)
    Individual policer configuration:
      Bandwidth:        1000 pps
      Burst:            1000 packets
      Priority:         low
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    FPC slot 1 information:
      Bandwidth: 100% (1000 pps), Burst: 100% (1000 packets), enabled

  Packet type: request (DHCPv4 DHCPREQUEST)
    Individual policer configuration:
      Bandwidth:        1000 pps
      Burst:            1000 packets
      Priority:         medium
```

```
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    FPC slot 1 information:
      Bandwidth: 100% (1000 pps), Burst: 100% (1000 packets), enabled

...
```

show ddos-protection protocols statistics

Syntax **show ddos-protection protocols <*protocol-group*> statistics <brief | detail | terse>**

Release Information Command introduced in Junos OS Release 11.2.

Description Display traffic statistics and DDoS policer violation statistics for all protocol groups or for a particular protocol group.

Options **none**—Display information for all protocol groups.

brief | detail | terse—(Optional) Display the specified level of output.

- **brief**—Display basic function information.
- **detail**—Add information to the **brief** output; it is identical to the output displayed when you choose no option. The **brief** and **detail** options display information for all protocol groups, which can be a long list.
- **terse**—Display the same level of information as the **brief** option but only for active protocol groups—groups that show traffic in the **Received (packets)** column.

protocol-group—(Optional) Display information for a particular protocol group. See show ddos-protection protocols for a list of available groups.

Required Privilege Level view

Related Documentation

- clear ddos-protection protocols on page 54
- show ddos-protection protocols on page 55
- show ddos-protection protocols culprit-flows
- show ddos-protection protocols flow-detection
- show ddos-protection protocols parameters on page 70
- show ddos-protection protocols violations on page 87

List of Sample Output

show ddos-protection protocols statistics on page 79
show ddos-protection protocols statistics brief on page 82
show ddos-protection protocols statistics terse on page 83
show ddos-protection protocols pppoe statistics on page 84
show ddos-protection protocols pppoe statistics brief on page 86

Output Fields Table 5 on page 78 lists the output fields for the **show ddos-protection protocols statistics** command. Output fields are listed in the approximate order in which they appear.

Table 5: show ddos-protection protocols statistics Output Fields

Field Name	Field Description	Level of Output
Protocol Group	Name of protocol group.	All levels
Packet type	Name of packet type in protocol group.	All levels
System-wide information	The following information collected for the router: • A message indicates whether the policer has been violated. • No. of FPCs currently receiving excess traffic—Number of cards that are currently in violation of a policer. • No. of FPCs that have received excess traffic—Number of cards that have at some point been in violation of a policer. • Violation first detected at—Timestamp of the first violation. • Violation last seen at—Timestamp of the last observed violation. • Duration of violation—Length of the violation. • Number of violations—Number of times the violation has occurred. • Received—Number of packets received at all card slots and the Routing Engine. • Dropped—Number of packets dropped regardless of where they were dropped. • Arrival rate—Current traffic rate for packets arriving from all cards and at the Routing Engine. • Max arrival rate—Highest traffic rate for packets arriving from all cards and at the Routing Engine.	**detail** none
Routing Engine information	The following information collected for the Routing Engine: • 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. • Violation first detected at—Timestamp of the first violation. • Violation last seen at—Timestamp of the last observed violation. • Duration of violation—Length of the violation. • Number of violations—Number of times the violation has occurred. • Received—Number of packets received at the Routing Engine from all cards. • Dropped—Number of packets dropped at the Routing Engine; includes packets dropped by the aggregate policer and by individual protocol policers. • Arrival rate—Current traffic rate for packets arriving at the Routing Engine from all cards. • Max arrival rate—Highest traffic rate for packets arriving at the Routing Engine from all cards. • Dropped by aggregate policer—Number of packets dropped by the aggregate policer. • Dropped by individual policers—Number of packets dropped by individual policer.	**detail** none

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

Field Name	Field Description	Level of Output
FPC slot information	The following information collected for the card in the indicated slot: • A message indicates whether the policer has been violated • Violation first detected at—Timestamp of the first violation • Violation last seen at—Timestamp of the last observed violation • Duration of violation—Length of the violation • Number of violations—Number of times the violation has occurred • Received—Number of packets received on the line card • Dropped—Number of packets dropped at the line card; includes packets dropped by the aggregate policer and by individual protocol policers • Arrival rate—Current traffic rate for packets arriving at the line card • Max arrival rate—Highest traffic rate for packets arriving at the line card • Dropped by this policer—Number of packets dropped by the individual policer • Dropped by aggregate policer—Number of packets dropped by the aggregate policer	**detail** none
Received (packets)	Number of packets of this packet type or protocol group received at all cards and the Routing Engine.	**brief terse**
Dropped (packets)	Number of packets dropped for this packet type or protocol group, regardless of where the packets were dropped.	**brief terse**
Rate (pps)	Highest observed traffic rate for this packet type or protocol group.	**brief terse**
Violation counts	Number of violations of the policer bandwidth.	**brief terse**
State	Violation state of the packet type: • **ok**—Policer has not been violated for this packet type • **viol**—Policer has been violated for this packet type	**brief terse**

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    Packet      Received        Dropped         Rate     Violation State
group       type        (packets)       (packets)       (pps)    counts
ipv4-uncls  aggregate   0               0               0        0         ok
ipv6-uncls  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
dhcpv4       aggregate    0            0            0       0       ok
dhcpv4       unclass..    0            0            0       0       ok
dhcpv4       discover     0            0            0       0       ok
dhcpv4       offer        0            0            0       0       ok
dhcpv4       request      0            0            0       0       ok
dhcpv4       decline      0            0            0       0       ok
dhcpv4       ack          0            0            0       0       ok
dhcpv4       nak          0            0            0       0       ok
dhcpv4       release      0            0            0       0       ok
dhcpv4       inform       0            0            0       0       ok
dhcpv4       renew        0            0            0       0       ok
dhcpv4       forcerenew   0            0            0       0       ok
dhcpv4       leasequery   0            0            0       0       ok
dhcpv4       leaseuna..   0            0            0       0       ok
dhcpv4       leaseunk..   0            0            0       0       ok
dhcpv4       leaseact..   0            0            0       0       ok
dhcpv4       bootp        0            0            0       0       ok
dhcpv4       no-msgtype   0            0            0       0       ok
dhcpv4       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-uncls   aggregate    241          0            0       0       ok
icmp         aggregate    20           0            0       0       ok
igmp         aggregate    55           0            0       0       ok
ospf         aggregate    956          0            0       0       ok
rsvp         aggregate    784          0            0       0       ok
ldp          aggregate    2984         0            0       0       ok
bgp          aggregate    312          0            0       0       ok
```

```
lacp        aggregate   1744          0             0        0        ok
stp         aggregate   9791          0             0        0        ok
arp         aggregate   19            0             0        0        ok
pvstp       aggregate   393           0             0        0        ok
mlp         aggregate   624774        0             0        0        ok
mlp         packets     1714371       223937        0        3        ok
mcast-copy  aggregate   3018038       0             0        0        ok
igmp-snoop  aggregate   43            0             0        0        ok
fw-host     aggregate   95547         0             0        0        ok
uncls       aggregate   10000         0             0        0        ok
```

show ddos-protection protocols pppoe statistics

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

  Packet type: aggregate
    System-wide information:
      Aggregate bandwidth is never violated
      Received:  60381200            Arrival rate:     4000 pps
      Dropped:   0                   Max arrival rate: 4002 pps
    Routing Engine information:
      Aggregate policer is never violated
      Received:  15095242            Arrival rate:     1001 pps
      Dropped:   0                   Max arrival rate: 1011 pps
        Dropped by individual policers: 0
    FPC slot 1 information:
      Aggregate policer is never violated
      Received:  60381200            Arrival rate:     4000 pps
      Dropped:   45287921            Max arrival rate: 4002 pps
        Dropped by individual policers: 45287921

  Packet type: padi
    System-wide information:
      Bandwidth is being violated!
        No. of FPCs currently receiving excess traffic: 1
        No. of FPCs that have received excess traffic:  1
        Violation first detected at: 2011-04-19 08:23:17 PDT
        Violation last seen at:      2011-04-19 12:34:48 PDT
        Duration of violation: 04:11:31 Number of violations: 1
      Received:  30190600            Arrival rate:     2000 pps
      Dropped:   22643960            Max arrival rate: 2001 pps
    Routing Engine information:
      Policer is never violated
      Received:  7547621             Arrival rate:     499 pps
      Dropped:   0                   Max arrival rate: 505 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Policer is currently being violated!
        Violation first detected at: 2011-04-19 08:23:17 PDT
        Violation last seen at:      2011-04-19 12:34:48 PDT
        Duration of violation: 04:11:31 Number of violations: 1
      Received:  30190600            Arrival rate:     2000 pps
      Dropped:   22643960            Max arrival rate: 2001 pps
        Dropped by this policer: 22643960
        Dropped by aggregate policer: 0

  Packet type: pado
    System-wide information:
      Bandwidth is never violated
      Received:  0                   Arrival rate:     0 pps
      Dropped:   0                   Max arrival rate: 0 pps
    Routing Engine information:
```

```
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0

Packet type: padr
  System-wide information:
    Bandwidth is being violated!
      No. of FPCs currently receiving excess traffic: 1
      No. of FPCs that have received excess traffic:  1
      Violation first detected at: 2011-04-19 08:23:17 PDT
      Violation last seen at:      2011-04-19 12:34:48 PDT
      Duration of violation: 04:11:31 Number of violations: 1
    Received:  30190600           Arrival rate:     2000 pps
    Dropped:   22643961           Max arrival rate: 2001 pps
  Routing Engine information:
    Policer is never violated
    Received:  7547621            Arrival rate:     501 pps
    Dropped:   0                  Max arrival rate: 506 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is currently being violated!
      Violation first detected at: 2011-04-19 08:23:17 PDT
      Violation last seen at:      2011-04-19 12:34:48 PDT
      Duration of violation: 04:11:31 Number of violations: 1
    Received:  30190600           Arrival rate:     2000 pps
    Dropped:   22643961           Max arrival rate: 2001 pps
      Dropped by this policer: 22643961
      Dropped by aggregate policer: 0

Packet type: pads
  System-wide information:
    Bandwidth is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
  Routing Engine information:
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0

Packet type: padt
  System-wide information:
    Bandwidth is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
  Routing Engine information:
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
```

```
  FPC slot 1 information:
    Policer is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
      Dropped by aggregate policer: 0

Packet type: padm
  System-wide information:
    Bandwidth is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
  :
    Policer is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
      Dropped by aggregate policer: 0

Packet type: padn
  System-wide information:
    Bandwidth is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
  :
    Policer is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
```

show ddos-protection protocols pppoe statistics brief

```
user@host> show ddos-protection protocols pppoe statistics brief
Protocol    Packet      Received        Dropped         Rate     Violation State
group       type        (packets)       (packets)       (pps)    counts
pppoe       aggregate   60901227        0               4000     0         ok
pppoe       padi        30450613        22838981        2000     1         viol
pppoe       pado        0               0               0        0         ok
pppoe       padr        30450614        22838977        2000     1         viol
pppoe       pads        0               0               0        0         ok
pppoe       padt        0               0               0        0         ok
pppoe       padm        0               0               0        0         ok
pppoe       padn        0               0               0        0         ok
```

show ddos-protection protocols violations

Syntax **show ddos-protection protocols <*protocol-group*> violations**

Release Information Command introduced in Junos OS Release 11.2.

Description Display information about DDoS policer violations for all protocol groups or for a particular protocol group.

Options **none**—Display information for all protocol groups.

protocol-group—(Optional) Name of a particular protocol group. See show ddos-protection protocols for a list of available groups.

Required Privilege Level view

Related Documentation

- clear ddos-protection protocols on page 54
- show ddos-protection protocols on page 55
- show ddos-protection protocols culprit-flows
- show ddos-protection protocols flow-detection
- show ddos-protection protocols parameters on page 70
- show ddos-protection protocols statistics on page 77

List of Sample Output

show ddos-protection protocols violations on page 88
show ddos-protection protocols dhcpv4 violations on page 88
show ddos-protection protocols pppoe violations on page 88

Output Fields Table 6 on page 87 lists the output fields for the **show ddos-protection protocols violations** command. Output fields are listed in the approximate order in which they appear.

Table 6: 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 6: 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

Syntax **show ddos-protection statistics**

Release Information Command introduced in Junos OS Release 11.2.

Description Display DDoS protection global statistics for bandwidth violations.

Options This command has no options.

Required Privilege Level view

Related Documentation
- clear ddos-protection protocols on page 54
- show ddos-protection protocols on page 55
- show ddos-protection version on page 90

List of Sample Output show ddos-protection statistics on page 89

Output Fields Table 7 on page 89 lists the output fields for the **show ddos-protection statistics** command. Output fields are listed in the approximate order in which they appear.

Table 7: show ddos-protection statistics Output Fields

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

Sample Output

show ddos-protection statistics

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

show ddos-protection version

Syntax **show ddos-protection version**

Release Information Command introduced in Junos OS Release 11.2.

Description Display the DDoS protection version and the total numbers of protocol groups and packet types that this version can be configured in this version.

Options This command has no options.

Required Privilege Level view

Related Documentation

- clear ddos-protection protocols on page 54
- show ddos-protection protocols on page 55
- show ddos-protection statistics on page 89

List of Sample Output show ddos-protection version on page 90

Output Fields Table 8 on page 90 lists the output fields for the **show ddos-protection version** command. Output fields are listed in the approximate order in which they appear.

Table 8: show ddos-protection version Output Fields

Field Name	Field Description
Version	Version number of the DDoS protection code.
Total protocol groups	Number of protocol groups configured with DDoS protection.
Total tracked packet types	Number of protocol packet types configured with DDoS protection.

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

CHAPTER 8

Acquiring Troubleshooting Information

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 94.

2. (Optional) Configure the number and size of trace logs.

   See "Configuring the Number and Size of DDoS Protection Log Files" on page 94.

3. (Optional) Configure user access to trace logs.

   See "Configuring Access to the DDoS Protection Log File" on page 95.

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 95.

5. (Optional) Configure flags to specify which events are logged.

   See "Configuring the DDoS Protection Tracing Flags" on page 96.

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.

Related Documentation

- Example: Configuring DDoS Protection on page 19

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 93

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 93

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 93

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 93

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 93

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 on page 98

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

Problem You have collected logs on your device and need to send them to Juniper Technical Support. This topic shows you how to compress the logs into a single file for each Routing Engine to more conveniently send the logs.

Solution You can compress all the log files in the **/var/log** directories of the master and backup (if present) Routing Engines into a single **tgz** file for each Routing Engine, which enables you to send the logs to JTAC in a convenient package. You can use either the CLI or the command shell to perform these tasks; because of its ease of use, only the CLI version is shown here.

1. Access the device through the management IP address or console, typically on the master Routing Engine, RE0.

   ```
   user@host>
   ```

2. Archive and compress all the log files on RE0 and put them in **/var/tmp**.

   ```
   user@host> file archive compress source /var/log/* destination /var/tmp/re0.tgz
   /usr/bin/tar: Removing leading `/' from member names
   ```

3. Confirm that the compressed archive file has been created.

   ```
   user@host> file list /var/tmp
   baseline-config.conf
   gres-tp
   idp_license_info
   install
   jinstall-12.2-20120328.0-domestic-signed.tgz
   krt_gencfg_filter.txt
   preinstall_boot_loader.conf
   re0.tgz
   rtsdb
   sec-download
   vi.recover
   ```

   On devices with a single Routing Engine, skip to Step 10.

4. Log in to the backup Routing Engine, RE1, and access the CLI.

NOTE: *1* is appended to the hostname in the prompt to signify that you are on RE1.

```
user@host> request routing-engine login backup
% cli
user@host11>
```

5. Archive and compress all the log files on RE1 and put them in **/var/tmp**.

```
user@host1> file archive compress source /var/log/* destination /var/tmp/re1.tgz
/usr/bin/tar: Removing leading `/' from member names
```

6. Confirm that the compressed archive file has been created.

```
user@host1> file list /var/tmp
baseline-config.conf
gres-tp
idp_license_info
install
jinstall-12.2-20120328.0-domestic-signed.tgz
krt_gencfg_filter.txt
preinstall_boot_loader.conf
re1.tgz
rtsdb
sec-download
vi.recover
%
```

7. Exit the remote login to the backup Routing Engine to return to the master Routing Engine. Note that the previously appended *1* is removed from the hostname in the prompt to signify that you are back on RE0.

```
user@host1> exit
rlogin: connection closed

user@host1>
```

8. Copy the compressed archive file from RE1 to RE0.

```
user@host> file copy re1:/var/tmp/re1.tgz /var/tmp
```

9. Confirm the presence of the copied file.

```
user@host> file list /var/tmp
baseline-config.conf
gres-tp
idp_license_info
install
jinstall-12.2-20120328.0-domestic-signed.tgz
krt_gencfg_filter.txt
preinstall_boot_loader.conf
re0.tgz
re1.tgz
rtsdb
sec-download
vi.recover
%
```

10. Copy the files directly from the master Routing Engine to any local host using FTP, SCP, JWEB, or (on some devices) a mounted USB.

Related Documentation

- Collecting Subscriber Access Logs Before Contacting Juniper Technical Support on page 96

CHAPTER 9

Troubleshooting Configuration Statements

traceoptions (DDoS)

Syntax

```
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 ddos-protection]

Release Information Statement introduced in Junos OS Release 11.2.

Description Define tracing operations for DDoS protection processes.

Options

file *filename*—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**.

files *number*—(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.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **config**—Trace configuration events.
- **events**—Trace all events.
- **gres**—Trace GRES events.
- **init**—Trace daemon initialization.
- **ipc**—Trace IPC events.
- **memory**—Trace memory management code.
- **protocol**—Trace DDoS protocol processing events.
- **rtsock**—Trace routing socket events.
- **signal**—Trace signal handling events.
- **socket**—Trace socket events.
- **state**—Trace state machine events.
- **timer**—Trace timer events.
- **ui**—Trace user interface events.

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

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

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

no-remote-trace—Disable remote tracing.

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

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

Syntax: ***size*****k** to specify KB, ***size*****m** to specify MB, or ***size*****g** 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

- Tracing DDoS Protection Operations on page 93

PART 5

Index

Index

Symbols

B

C

D