



---

Junos<sup>®</sup> OS

# DDoS Protection Configuration Guide

Release  
11.2



---

Published: 2011-05-11

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

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

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

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

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

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

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

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

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

#### *Junos® OS DDoS Protection Configuration Guide*

Copyright © 2011, Juniper Networks, Inc.  
All rights reserved.

Revision History  
May 2011—R1 Junos OS 11.2

The information in this document is current as of the date listed in the revision history.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The 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

**READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE.** BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14 (ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).



# Abbreviated Table of Contents

<b>Part 1</b>	<b>Distributed Denial-of-Service (DDoS) Protection</b>	
<b>Chapter 1</b>	<b>DDoS Overview .....</b>	<b>3</b>
<b>Chapter 2</b>	<b>Configuring DDoS Protection .....</b>	<b>9</b>
<b>Chapter 3</b>	<b>DDoS Protection Configuration Hierarchy .....</b>	<b>27</b>
<b>Chapter 4</b>	<b>DDoS Protection Configuration Statements .....</b>	<b>29</b>
<b>Part 2</b>	<b>Indexes</b>	
	<b>Index .....</b>	<b>49</b>
	<b>Index of Statements and Commands .....</b>	<b>51</b>





# Table of Contents

<b>Part 1</b>	<b>Distributed Denial-of-Service (DDoS) Protection</b>	
<b>Chapter 1</b>	<b>DDoS Overview</b>	<b>3</b>
	Distributed Denial of Service (DDoS) Protection Overview	3
	Policer Types and Packet Priorities	4
	Policer Hierarchy	5
<b>Chapter 2</b>	<b>Configuring DDoS Protection</b>	<b>9</b>
	Configuring Protection Against DDoS Attacks	9
	Disabling DDoS Protection Policers and Logging Globally	10
	Configuring DDoS Protection Policers for Individual Packet Types	10
	Tracing DDoS Protection Operations	12
	Configuring the DDoS Protection Trace Log Filename	13
	Configuring the Number and Size of DDoS Protection Log Files	13
	Configuring Access to the DDoS Protection Log File	14
	Configuring a Regular Expression for DDoS Protection to Be Logged	14
	Configuring the DDoS Protection Tracing Flags	14
	Verifying and Managing DDoS Protection	15
	Example: Configuring DDoS Protection	16
<b>Chapter 3</b>	<b>DDoS Protection Configuration Hierarchy</b>	<b>27</b>
	[edit system ddos-protection] Hierarchy Level	27
<b>Chapter 4</b>	<b>DDoS Protection Configuration Statements</b>	<b>29</b>
	bandwidth (DDoS)	29
	bandwidth-scale (DDoS)	30
	burst (DDoS)	30
	burst-scale (DDoS)	31
	bypass-aggregate (DDoS)	31
	ddos-protection (DDoS)	32
	disable-fpc (DDoS)	33
	disable-logging (DDoS)	33
	disable-routing-engine (DDoS)	34
	fpc (DDoS)	34
	global (DDoS)	35
	priority (DDoS)	35
	protocols (DDoS)	36
	recover-time (DDoS)	43
	traceoptions (DDoS)	44
	violation (DDoS)	45

Part 2	Indexes	
	Index .....	49
	Index of Statements and Commands .....	51

# List of Figures

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



## PART 1

# Distributed Denial-of-Service (DDoS) Protection

- DDoS Overview on page 3
- Configuring DDoS Protection on page 9
- DDoS Protection Configuration Hierarchy on page 27
- DDoS Protection Configuration Statements on page 29



## CHAPTER 1

# DDoS Overview

- Distributed Denial of Service (DDoS) Protection Overview on page 3

### Distributed Denial of Service (DDoS) Protection Overview

---

A denial-of-service attack is any attempt to deny valid users access to network or server resources by using up all the resources of the network element or server. Distributed denial-of-service attacks involve an attack from multiple sources, enabling a much greater amount of traffic to attack the network. The attacks typically use network protocol control packets to trigger a large number of exceptions in the network.

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 facilitates a customized network control traffic profile. Protection and monitoring persists across graceful Routing Engine switchover (GRES) and unified in-service-software-upgrade (ISSU) switchovers. Protection is not diminished as the number of subscribers increases.

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

The policers at the Trio MPC are the first line of protection. Control traffic is dropped when it violates the policer by exceeding the configured or default rate limit. Each violation generates a notification to alert operators about a possible attack. The violation is counted, the time that the violation starts is noted, and the time of the last observed violation is noted. When the traffic rate drops below the bandwidth violation threshold, a recovery timer determines when the traffic flow is considered to have returned to normal. If no further violation occurs before the timer expires, the violation state is cleared and a notification is generated.

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



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

---

## Policer Types and Packet Priorities

DDoS protection includes two types of policers:

- An *aggregate policer* is applied to the complete set of packet types that belong to a protocol group. For example, you can configure an aggregate policer that applies to all PPPoE control packet types or to all DHCPv4 control packet types. You can specify bandwidth and burst limits, scale the bandwidth and burst limits, and set a traffic priority for aggregate policers. An aggregate policer is available for all protocol groups. Aggregate policers are supported by all protocol groups.
- An *individual policer*, also referred to as a *packet-type policer*, is allocated for each control packet type within a protocol group. For example, you can configure a policer for one or more types of PPPoE control packets. You can specify bandwidth and burst limits, scale the bandwidth and burst limits, and set a traffic priority for packet-type policers. Individual policers are not available for all protocol groups. See **protocols** for a list of protocol groups that have individual policers.

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

Each packet type within a protocol group has a default, configurable priority: low, medium, or high. Each control packet competes with other packets for the bandwidth within the limit imposed by its aggregate policer based on the priority configured for each packet type in the protocol group. Within the aggregate policer, burst size scaling is applied to the individual policers. Burst size traffic is doubled for high-priority traffic and halved for low-priority traffic.

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.

For example, consider how you might configure packet types within the PPPoE protocol group. Suppose you configure individual policers for PADI and PADT packets. In addition, you configure 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. You might assign high priority to the PADT packets and low priority to the PADI packets. If PADT packets use the bandwidth up to the limit imposed by the aggregate policer, then all PADI packets are dropped.



## Policer Hierarchy

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

Figure 1: Policer Hierarchy for PPPoE Packets

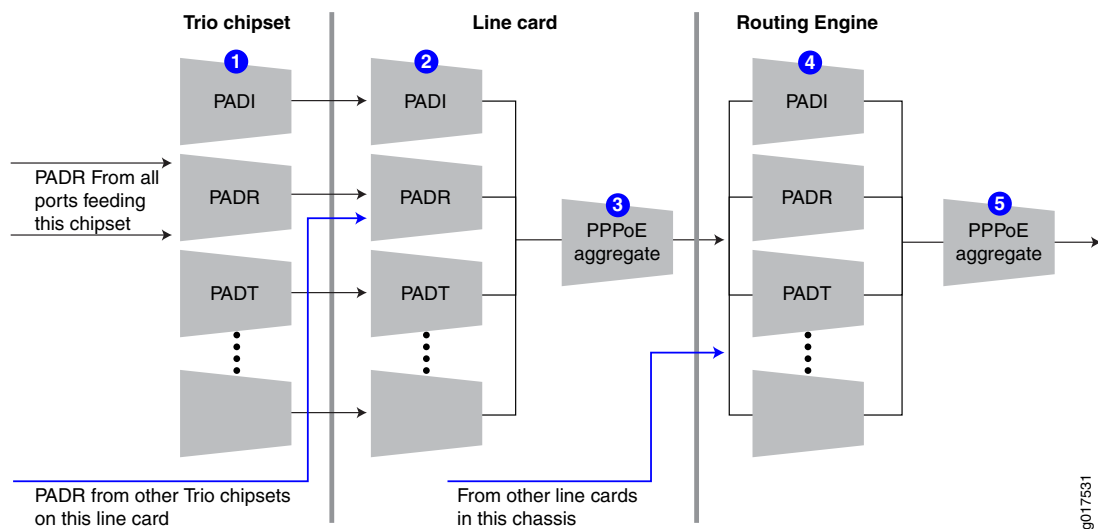
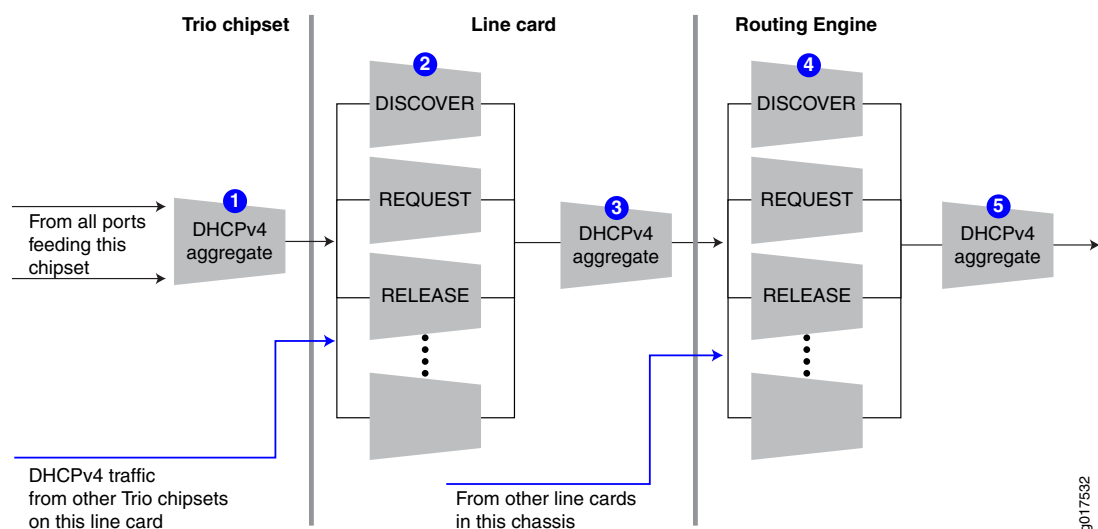


Figure 2: Policer Hierarchy for DHCPv4 Packets



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

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

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

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

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

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

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

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

1. PADR packets, for example, are evaluated at the first policer on the Trio chipset to determine whether they are within the bandwidth limits. PADR packets that exceed the limit are dropped.
2. All PADR packets that pass the policer on all Trio chipsets on the Trio MPC are next evaluated by the line card individual policer. PADR packets that exceed the limit are dropped.

3. All PADR packets that pass the line card individual policer proceed to the line card aggregate policer. PADR packets that exceed the limit are dropped.
4. All PADR packets that are passed by the line card aggregate policers on all Trio MPCs on the router proceed to the Routing Engine individual policer. PADR packets that exceed the limit are dropped.
5. Finally, all PADR packets that are passed by the Routing Engine individual policer proceed to the Routing Engine aggregate policer. PADR packets that exceed the limit are dropped. PADR packets that are not dropped here are passed along as safe, normal traffic.

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

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

You can apply a scaling factor for both the bandwidth limit and the burst limit at the line card. This enables you to fine-tune the traffic limits for each slot. For example, suppose the individual policer sets the PADI packet bandwidth to 1000 pps and the burst size to 50,000 packets. You can reduce the traffic limit for PADI packets on any line card by specifying the slot number and scaling factor. A bandwidth scaling factor of 20 for slot 5 reduces the traffic in this example to 20 percent of 1000 pps, or 200 pps for the line card in that slot. Similarly, a burst scaling factor of 50 for that slot reduces the burst size by 50 percent to 25,000 packets. By default, scaling factors are set to 100 so traffic can pass through at 100 percent of the rate limit.

**Related  
Documentation**

- [Configuring Protection Against DDoS Attacks on page 9](#)



## CHAPTER 2

# Configuring DDoS Protection

- Configuring Protection Against DDoS Attacks on page 9
- Disabling DDoS Protection Policers and Logging Globally on page 10
- Configuring DDoS Protection Policers for Individual Packet Types on page 10
- Tracing DDoS Protection Operations on page 12
- Configuring the DDoS Protection Trace Log Filename on page 13
- Configuring the Number and Size of DDoS Protection Log Files on page 13
- Configuring Access to the DDoS Protection Log File on page 14
- Configuring a Regular Expression for DDoS Protection to Be Logged on page 14
- Configuring the DDoS Protection Tracing Flags on page 14
- Verifying and Managing DDoS Protection on page 15
- Example: Configuring DDoS Protection on page 16

## 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 entire protocol group. DDoS logging is enabled by default, but you can disable it globally for all DDoS events. You can also fine-tune monitoring of DDoS events by configuring tracing operations.



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

To configure DDoS protection:

1. (Optional) Configure global DDoS settings.  
See “Disabling DDoS Protection Policers and Logging Globally” on page 10.
2. (Optional) Configure DDoS settings for individual packet types.

See “Configuring DDoS Protection Policers for Individual Packet Types” on page 10.

3. (Optional) Configure tracing for DDoS operations.

See “Tracing DDoS Protection Operations” on page 12.

---

## Disabling DDoS Protection Policers and Logging Globally

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

DDoS logging is also enabled by default. You can disable all DDoS event logging for all protocol groups and packet types across the router.

To configure global DDoS settings:

1. (Optional) Disable line card policers.

```
[edit system ddos-protection global]  
user@host# set disable-fpc
```

2. (Optional) Disable Routing Engine policers.

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

3. (Optional) Disable event logging.

```
[edit system ddos-protection global]  
user@host# set disable-logging
```

**Related Documentation**

- Configuring Protection Against DDoS Attacks on page 9

---

## Configuring DDoS Protection Policers for Individual Packet Types

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

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

You can disable a packet type’s policer at either the Routing Engine or at a specified line card. You can also disable monitoring of all DDoS violations.



**NOTE:** DDoS protection is enabled by default. You can view the default values for all protocol group aggregate policers and individual packet type policers before you make configuration changes. To do so, from operational mode, enter the `show ddos-protection protocols parameters` command.

To configure individual, packet-level DDoS settings:

1. Specify the protocol group.
 

```
[edit system ddos-protection protocols]
user@host# set protocol-group
```
2. Specify the packet type or the combination of all packet types in the group.
 

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

or

```
[edit system ddos-protection protocols protocol-group]
user@host# set aggregate
```
3. (Optional) Configure the maximum traffic rate the policer allows for the packet type.
 

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set bandwidth packets-per-second
```
4. (Optional) Configure the maximum number of packets of the packet type that the policer allows in a burst of traffic.
 

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set burst size
```
5. (Optional) Set the traffic priority.
 

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set priority level
```
6. (Optional) Configure how much time must pass since the last violation before the traffic flow is considered to have recovered from the attack.
 

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set recover-time seconds
```
7. (Optional) Bypass the aggregate policer configuration. This is relevant only when an aggregate policer is configured for the protocol group.
 

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set bypass-aggregate
```
8. (Optional) Disable the Routing Engine policer for only this packet type. This setting overrides the global configuration.
 

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set disable-routing-engine
```
9. (Optional) Disable logging of DDoS violations.
 

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

10. (Optional) Configure packet-level settings on a single line card.

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

11. (Optional) Scale the policer bandwidth on the line card.

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

12. (Optional) Scale the policer burst size on the line card.

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

13. (Optional) Disable the line card policer.

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

**Related  
Documentation**

- [Configuring Protection Against DDoS Attacks](#) on page 9
- For a list of supported protocol groups and packet types, see [protocols](#) on page 36.

---

## 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 called **ddosd** located in the **/var/log** directory. You cannot change the directory (**/var/log**) in which trace files are located.
2. When the file **ddosd** reaches 128 kilobytes (KB), it is renamed **ddosd.0**, then **ddosd.1**, and finally **ddosd.2**, until there are three trace files. Then the oldest trace file (**ddosd.2**) 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. Configure a trace log filename.  
See “Configuring the DDoS Protection Trace Log Filename” on page 13.
2. Configure the number and size of trace logs.  
See “Configuring the Number and Size of DDoS Protection Log Files” on page 13.



3. Configure user access to trace logs.  
See “Configuring Access to the DDoS Protection Log File” on page 14.
4. Configure a regular expression to filter the information to be included in the trace log.  
See “Configuring a Regular Expression for DDoS Protection to Be Logged” on page 14.
5. Configure flags to specify which events are logged.  
See “Configuring the DDoS Protection Tracing Flags” on page 14.

## 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 12
- **traceoptions** on page 44

## Configuring the Number and Size of DDoS Protection Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed **filename.0**, then **filename.1**, and finally **filename.2**, until there are three trace files. Then the oldest trace file (**filename.2**) 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 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 renamed **filename.0**, and a new file called **filename** is created. When the new **filename** reaches 2 MB, **filename.0** is renamed **filename.1** and **filename** is renamed **filename.0**. This process repeats until there are 20 trace files. Then the oldest file (**filename.19**) is overwritten by the newest file (**filename.0**).

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 12
- **traceoptions** on page 44

## 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 12
- [traceoptions on page 44](#)

## Configuring a Regular Expression for DDoS Protection to Be Logged

---

By default, the trace operation output includes all lines 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 12
- [traceoptions on page 44](#)

## Configuring the DDoS Protection Tracing Flags

---

By default, only important events are logged. You can specify which trace operations are logged by including specific tracing flags. The following table describes the flags that you can include.

Flag	Description
all	Trace all operations.

---

Flag	Description
<b>config</b>	Trace configuration events.
<b>events</b>	Trace all events.
<b>gres</b>	Trace GRES events.
<b>init</b>	Trace daemon initialization.
<b>memory</b>	Trace memory management code.
<b>protocol</b>	Trace DDoS protocol processing events.
<b>rt-sock</b>	Trace routing socket events.
<b>signal</b>	Trace signal handling events.
<b>state</b>	Trace state machine events.
<b>timer</b>	Trace timer events.
<b>ui</b>	Trace user interface events.

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 12
- traceoptions on page 44

## Verifying and Managing DDoS Protection

**Purpose** View or clear information about DDoS configurations, states, and statistics.

**Action** • To display the DDoS policer configuration, violation state, and statistics for all packet types in all protocol groups:

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

If you issue the command before you make any configuration changes, the default policer values are displayed.

- To display the DDoS policer configuration, violation state, and statistics for a particular packet type in a particular protocol group:

```
user@host> show ddos-protection protocols protocol-group packet-type
```

- To display only the number of DDoS policer violations for all protocol groups:

**user@host> show ddos-protection protocols violations**

- To display a table of the DDoS configuration for all packet types in all protocol groups:

**user@host> show ddos-protection protocols parameters brief**

- To display a complete list of packet statistics and DDoS violation statistics for all packet types in all protocol groups:

**user@host> show ddos-protection protocols statistics detail**

- To display global DDoS violation statistics:

**user@host> show ddos-protection statistics**

- To display the DDoS version number:

**user@host> show ddos-protection version**

- To clear DDoS statistics for all packet types in all protocol groups:

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

- To clear DDoS statistics for all packet types in a particular protocol group:

**user@host> clear ddos-protection protocols statistics *protocol-group***

- To clear DDoS statistics for a particular packet type in a particular protocol group:

**user@host> clear ddos-protection protocols statistics *protocol-group packet-type***

- To clear DDoS violation states for all packet types in all protocol groups:

**user@host> clear ddos-protection protocols state**

- To clear DDoS violation states for all packet types in a particular protocol group:

**user@host> clear ddos-protection protocols state *protocol-group***

- To clear DDoS violation states for a particular packet type in a particular protocol group:

**user@host> clear ddos-protection protocols state *protocol-group packet-type***

**Related  
Documentation**

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

---

## Example: Configuring DDoS Protection

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

- Requirements on page 17
- Overview on page 17
- Configuration on page 17
- Verification on page 19

## Requirements

DDoS protection is supported only for MX Series routers that have only Trio MPCs installed. If the router has other cards in addition to Trio MPCs, the CLI accepts the configuration but the other cards are not protected and therefore the router is not protected.

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 an entire protocol group and for particular control packet types within a protocol group, configuring an aggregate policer for a protocol group and bypassing that policer for a particular control packet type, and specifying trace options for DDoS operations.

This example does not show all possible configuration choices.

## Configuration

**CLI Quick Configuration** To quickly configure DDoS protection for protocol groups and particular control packet types, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
[edit]
edit system
set ddos-protection protocols dhcpv4 aggregate bandwidth 669
set ddos-protection protocols dhcpv4 aggregate burst 6000
set ddos-protection protocols dhcpv4 discover bandwidth 100
set ddos-protection protocols dhcpv4 discover recover-time 200
set ddos-protection protocols dhcpv4 discover burst 300
set ddos-protection protocols dhcpv4 offer priority medium
set ddos-protection protocols dhcpv4 offer bypass-aggregate
set ddos-protection protocols dhcpv4 offer fpc 1 bandwidth-scale 80
set ddos-protection protocols dhcpv4 offer fpc 1 burst-scale 75
set ddos-protection protocols pppoe aggregate bandwidth 800
set ddos-protection traceoptions file ddos-trace size 10m
set ddos-protection traceoptions flag all
top
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure DDoS protection:

1. Specify a protocol group.

- [edit system ddos-protection protocols]  
user@host# set dhcpv4
2. Configure the maximum traffic rate for the DHCPv4 aggregate policer; that is, for the combination of all DHCPv4 packets.  
  
[edit system ddos-protection protocols dhcpv4]  
user@host# set aggregate bandwidth 669
  3. Configure the maximum burst rate for the DHCPv4 aggregate policer.  
  
[edit system ddos-protection protocols dhcpv4]  
user@host# set aggregate burst 6000
  4. Configure the maximum traffic rate for the DHCPv4 policer for discover packets.  
  
[edit system ddos-protection protocols dhcpv4]  
user@host# set discover bandwidth 100
  5. Decrease the recover time for violations of the DHCPv4 discover policer.  
  
[edit system ddos-protection protocols dhcpv4]  
user@host# set discover recover-time 200
  6. Configure the maximum burst rate for the DHCPv4 discover policer.  
  
[edit system ddos-protection protocols dhcpv4]  
user@host# set discover burst 300
  7. Increase the priority for DHCPv4 offer packets.  
  
[edit system ddos-protection protocols dhcpv4]  
user@host# set offer priority medium
  8. Prevent offer packets from being included in the aggregate bandwidth; that is, offer packets will not contribute towards the combined DHCPv4 traffic to determine whether the aggregate bandwidth is exceeded. However, the offer packets are still included in traffic rate statistics.  
  
[edit system ddos-protection protocols dhcpv4]  
user@host# set offer bypass-aggregate
  9. Reduce the bandwidth and burst size allowed before violation is declared for the DHCPv4 offer policer on the Trio MPC in slot 1.  
  
[edit system ddos-protection protocols dhcpv4]  
user@host# set offer fpc 1 bandwidth-scale 80  
user@host# set offer fpc 1 burst-scale 75
  10. Configure the maximum traffic rate for the PPPoE aggregate policer, that is, for the combination of all PPPoE packets.  
  
[edit system ddos-protection protocols dhcpv4]  
user@host# up  
[edit system ddos-protection protocols]  
user@host# set pppoe aggregate bandwidth 800
  11. Configure tracing for all DDoS protocol processing events.  
  
[edit system ddos-protection traceoptions]  
user@host# set file ddos-log  
user@host# set file size 10m  
user@host# set flag all

**Results** From configuration mode, confirm your configuration by entering the **show ddos-protection** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit system]
user@host# show ddos-protection
traceoptions {
  file ddos-trace size 10m;
  flag all;
}
protocols {
  pppoe {
    aggregate {
      bandwidth 800;
    }
  }
  dhcpv4 {
    aggregate {
      bandwidth 669;
      burst 6000;
    }
    discover {
      bandwidth 100;
      burst 300;
      recover-time 200;
    }
    offer {
      priority medium;
      fpc 1 {
        bandwidth-scale 80;
        burst-scale 75;
      }
      bypass-aggregate;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

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

- Verifying the DHCPv4 DDoS Protection Configuration and Operation on page 19
- Verifying the PPPoE DDoS Configuration on page 22

### 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.

**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:
  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:
  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% (500 packets), enabled
  Policer is no longer being violated
  Violation first detected at: 2011-03-10 06:28:35 PST
  Violation last seen at: 2011-03-10 06:28:55 PST
  Duration of violation: 00:00:20 Number of violations: 1
  Received: 47949           Arrival rate: 0 pps
  Dropped: 11819           Max arrival rate: 671 pps
  Dropped by this policer: 11819
  Dropped by aggregate policer: 0

```

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

```

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

Packet type: offer (DHCPv4 DHCP OFFER)
Individual policer configuration:
  Bandwidth: 1000 pps
  Burst: 1000 packets
  Priority: medium
  Recover time: 300 seconds
  Enabled: Yes
  Bypass aggregate: Yes
System-wide information:
  Bandwidth is never violated
  Received: 0           Arrival rate: 0 pps
  Dropped: 0           Max arrival rate: 0 pps
Routing Engine information:
  Policer is never violated
  Received: 0           Arrival rate: 0 pps
  Dropped: 0           Max arrival rate: 0 pps
  Dropped by aggregate policer: 0
FPC slot 1 information:
  Bandwidth: 80% (800 pps), Burst: 75% (750 packets), enabled
  Policer is never violated
  Received: 0           Arrival rate: 0 pps
  Dropped: 0           Max arrival rate: 0 pps
  Dropped by aggregate policer: 0

```

**Meaning** The output of these commands lists the policer configuration and traffic statistics for the DHCPv4 aggregate, discover, and offer policers. Alternatively, you could have entered the **show ddos-protection protocols dhcpv4** command to display this information for all DHCPv4 packet types.

Verify that the values shown in the **Aggregate policer configuration** and **Individual policer configuration** sections match what you configured for bandwidth, burst, priority, recover time, and bypass-aggregate. Default values are listed for all policers that you did not configure.

The **System-wide information** section shows the total of all DHCPv4 traffic statistics and policer violations recorded across all line cards and at the Routing Engine. The **Routing engine information** section shows the traffic statistics and policer violations recorded at

the Routing Engine. The **FPC slot 1 information** section shows the traffic statistics and policer violations recorded only at the line card in slot 1.

In addition to configuration information, the output for the aggregate policer in this example shows the following information:

- A single violation has occurred, and it took place on the line card in slot 1. Timestamps report when the violation was first and last detected, and the duration of the violation. The aggregate policer is not currently being violated.
- 71,064 DHCPv4 packets of all types have been received across all line cards and the Routing Engine; 23,115 of these packets have been dropped by the aggregate policer, without reference to where they were dropped. All 71,064 DHCPv4 packets were received at the line card in slot 1. The line card dropped 23,115 packets at the aggregate policer and 11,819 packets in individual policers. At the Routing Engine itself, 47,949 packets have been received and none dropped.

In addition to configuration information, the output for the DHCPv4 discover packet policer in this example shows the following information:

- A single violation has occurred, and it took place on the line card in slot 1. Timestamps report when the violation was first and last detected, and the duration of the violation. The individual policer is not currently being violated.
- 47,949 DHCPv4 discover packets have been received across all line cards and the Routing Engine; 11,819 of these packets have been dropped by the individual policer, without reference to where they were dropped. All 47,949 discover packets were received at the line card in slot 1. The line card dropped 11,819 packets at the individual policer and no packets at the aggregate policer. At the Routing Engine itself, 36,130 packets have been received and none dropped.

In addition to configuration information, the output for the DHCPv4 offer packet policer in this example shows the following information:

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

### 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:
  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:
  Policer is never violated
  Received: 10287753         Arrival rate: 500 pps
  Dropped: 0                Max arrival rate: 502 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: 2011-03-10 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.

In addition to configuration information, the output of the **show ddos-protection protocols pppoe padi** command in this example shows the following information:

- The **System-wide information** section shows the total of all PPPoE PADI traffic statistics and policer violations recorded across all line cards and at the Routing Engine. A single violation has occurred, it is still taking place, and the violation has been seen on only a single line card. Timestamps report when the violation was first and last detected, and the duration of the violation.

704,832,908 PPPoE PADI packets have been received across all line cards and the Routing Engine; 660,788,548 of these packets have been dropped without reference to where they were dropped.

- The **Routing engine information** section shows the PADI traffic statistics and policer violations recorded at the Routing Engine. In this example, the section reports that 39,950,330 PADI packets have been received and that no violation of the policer at this level has occurred.
- The **FPC slot 3 information** section shows the PADI traffic statistics and policer violations recorded only at the line card in slot 3. In this example, the section reports that one violation has occurred, it is still taking place, and has lasted over a day.

All 704,832,908 PADI packets were received at the line card in slot 3. The line card dropped a total of 664,882,578 packets. Of the packets dropped, 660,788,548 were dropped by the individual PADI policer and 4,094,030 packets were dropped at the aggregate policer. The difference between the packets received and dropped at the line card 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.

In addition to configuration information, 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 a single PADR violation has occurred, it is still taking place, and the violation has been seen on only a single line card. Timestamps report when the violation was first and last detected, and the duration of the violation.

494,663,595 PPPoE PADR packets have been received across all line cards and the Routing Engine; 484,375,900 of these packets have been dropped without reference to where they were dropped.

- The **Routing engine information** section shows the PADR traffic statistics and policer violations recorded at the Routing Engine. In this example, the section reports that 10,287,753 PADR packets have been received and that no violation of the policer at this level has occurred.
- The **FPC slot 1 information** section shows the PADR traffic statistics and policer violations recorded only at the line card in slot 1. In this example, the section reports that one violation has occurred, it is still taking place, and has lasted over 5 hours.

All 494,663,595 PADR packets were received at the line card in slot 1. The line card dropped a total of 484,375,900 packets. All the packets were dropped by the individual policer; none were dropped by the aggregate policer. In this example, only the line card in slot 1 received any PADI packets. The difference between the packets received and dropped at the line card matches the number received at the Routing Engine.



**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 this is to illustrate how policer violations are reported for individual line cards.

#### Related Documentation

- Distributed Denial of Service (DDoS) Protection Overview on page 3
- Configuring Protection Against DDoS Attacks on page 9



## CHAPTER 3

# DDoS Protection Configuration Hierarchy

- [\[edit system ddos-protection\] Hierarchy Level on page 27](#)

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

---

```
system {
  ddos-protection {
    global {
      disable-fpc;
      disable-logging;
      disable-routing-engine;
    }
    protocols protocol-group (aggregate | packet-type) {
      bandwidth packets-per-second;
      burst size;
      bypass-aggregate;
      disable-routing-engine;
      fpc slot-number {
        bandwidth-scale percentage;
        burst-scale percentage;
        disable-fpc;
      }
      priority level;
      recover-time seconds;
      violation {
        disable-logging;
      }
    }
    traceoptions{
      file filename <files number> <match regular-expression > <size maximum-file-size>
        <world-readable | no-world-readable>;
      flag flag;
      level (all | error | info | notice | verbose | warning);
      no-remote-trace;
    }
  }
}
```

**Related Documentation** • [Configuring Protection Against DDoS Attacks on page 9](#)





## CHAPTER 4

# DDoS Protection Configuration Statements

### bandwidth (DDoS)

---

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

## bandwidth-scale (DDoS)

---

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

## burst (DDoS)

---

<b>Syntax</b>	<code>burst <i>size</i>;</code>
<b>Hierarchy Level</b>	[edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> )]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	(MX Series routers with Trio MPCs only) Configure the DDoS burst limit; the maximum number of packets of the packet type that is allowed in a burst of traffic. When this value is exceeded, a violation is declared.
<b>Options</b>	<b><i>size</i></b> —Number of packets that are allowed in a burst for the packet type. <b>Range:</b> 1 through 100,000 packets <b>Default:</b> The default burst value varies by packet type. You can view the default values for all packet types on an unconfigured router by entering the <b>show ddos-protection protocols parameters brief</b> command from operational mode.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring DDoS Protection Policers for Individual Packet Types on page 10</li></ul>

## burst-scale (DDoS)

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

## bypass-aggregate (DDoS)

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

## ddos-protection (DDoS)

<b>Syntax</b>	<pre> ddos-protection   global {     disable-fpc;     disable-logging;     disable-routing-engine;   }   protocols <i>protocol-group</i> (aggregate   <i>packet-type</i>) {     bandwidth <i>packets-per-second</i>;     burst <i>size</i>;     bypass-aggregate;     disable-routing-engine;     fpc <i>slot-number</i> {       bandwidth-scale <i>percentage</i>;       burst-scale <i>percentage</i>;       disable-fpc;     }     priority <i>level</i>;     recover-time <i>seconds</i>;     violation {       disable-logging;     }   }   traceoptions{     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;       &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;     level (all   error   info   notice   verbose   warning);     no-remote-trace;   } </pre>
<b>Hierarchy Level</b>	[edit system]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	<p>(MX Series routers with Trio MPCs only) Configure DDoS policers.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Protection Against DDoS Attacks on page 9</li> </ul>

## disable-fpc (DDoS)

<b>Syntax</b>	disable-fpc;
<b>Hierarchy Level</b>	[edit system ddos-protection global], [edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> ) fpc <i>slot-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	(MX Series routers with Trio MPCs only) Disable DDoS policers for debugging purposes on the card in the specified slot for a particular packet type within a protocol group or globally for all cards and all packet types in all protocols. This statement does not affect the state of the Routing Engine policers.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Disabling DDoS Protection Policers and Logging Globally on page 10</li> <li>Configuring DDoS Protection Policers for Individual Packet Types on page 10</li> </ul>

## disable-logging (DDoS)

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

## disable-routing-engine (DDoS)

---

<b>Syntax</b>	disable-routing-engine;
<b>Hierarchy Level</b>	[edit system ddos-protection global], [edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> )
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	(MX Series routers with Trio MPCs only) Disable DDoS Routing Engine policers for debugging purposes for all packet types in all protocols or for a particular packet type within a protocol group. This statement does not affect the state of the line card policers.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Disabling DDoS Protection Policers and Logging Globally on page 10</li></ul>

## fpc (DDoS)

---

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

## global (DDoS)

---

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

## priority (DDoS)

---

<b>Syntax</b>	<code>priority <i>level</i>;</code>
<b>Hierarchy Level</b>	[edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> )]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	<p>(MX Series routers with Trio MPCs only) Configure the priority for the packet type within the parent protocol group. In the event of downstream traffic congestion, high priority packets are provided bandwidth before medium priority packets. In turn, medium priority packets are provided bandwidth before low priority packets. Packets are dropped when there is insufficient available bandwidth.</p>
<b>Options</b>	<i>level</i> —Priority of the packet type, low, medium, or high.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring DDoS Protection Policers for Individual Packet Types on page 10</li> </ul>

## protocols (DDoS)

---

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

**Hierarchy Level**    [edit system ddos-protection]

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

**Description**    (MX Series routers with Trio MPCs only) Configure DDoS policers for all packet types within a protocol group or for a particular packet type within a protocol group.

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

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

- **dhcpv4**—The following packet types are available for DHCPv4 traffic:

- **ack**—DHCPACK packets.
- **bad-packets**—DHCPv4 packets with bad formats.
- **bootp**—DHCPBOOTP packets.
- **decline**—DHCPDECLINE packets.
- **discover**—DHCPDISCOVER packets.
- **force-renew**—DHCPFORCERENEW packets.
- **inform**—DHCPINFORM packets.
- **lease-active**—DHCPLEASEACTIVE packets.
- **lease-query**—DHCPLEASEQUERY packets.
- **lease-unassigned**—DHCPLEASEUNASSIGNED packets.
- **lease-unknown**—DHCPLEASEUNKNOWN packets.



- **nak**—DHCPNAK packets.
- **no-message-type**—DHCP packets that are missing the message type.
- **offer**—DHCP OFFER packets.
- **release**—DHCP RENEW packets.
- **renew**—DHCP RENEW packets.
- **request**—DHCP REQUEST packets.
- **unclassified**—All unclassified packets in the protocol group.
- **dhcpv6**—The following packet types are available for DHCPv6 traffic:
  - **advertise**—ADVERTISE packets.
  - **confirm**—CONFIRM packets.
  - **decline**—DECLINE packets.
  - **information-request**—INFORMATION-REQUEST packets.
  - **leasequery**—LEASEQUERY packets.
  - **leasequery-data**—LEASEQUERY-DATA packets.
  - **leasequery-done**—LEASEQUERY-DONE packets.
  - **leasequery-reply**—LEASEQUERY-REPLY packets.
  - **rebind**—REBIND packets.
  - **reconfigure**—RECONFIGURE packets.
  - **relay-forward**—RELAY-FORWARD packets.
  - **relay-reply**—RELAY-REPLY packets.
  - **release**—RELEASE packets.
  - **renew**—RENEW packets.
  - **reply**—REPLY packets.
  - **request**—REQUEST packets.
  - **solicit**—SOLICIT packets.
  - **unclassified**—All unclassified packets in the protocol group.
- **ip-fragments**—The following packet types are available for IP fragments:
  - **first-fragment**—First IP fragment.
  - **trail-fragment**—Last IP fragment.

- **ip-options**—The following packet types are available for IP option traffic:
  - **router-alert**—Router alert options packets.
  - **unclassified**—All unclassified packets in the protocol group.
- **ipv4-unclassified**—All unclassified host-bound IPv4 traffic.
- **ipv6-unclassified**—All unclassified host-bound IPv6 traffic.
- **mlp**—The following MLP packet types are available:
  - **aging-exception**—MLP aging exception packets.
  - **packets**—MLP packets.
  - **unclassified**—All unclassified packets in the protocol group.
- **ppp**—The following PPP packet types are available:
  - **authentication**—PPP authentication protocol packets.
  - **ipcp**—IP Control Protocol packets.
  - **ipv6cp**—IPv6 Control Protocol packets.
  - **isis**—IS-IS packets.
  - **lcp**—Link Control Protocol packets.
  - **mplscp**—MPLS Control Protocol packets.
  - **unclassified**—All unclassified packets in the protocol group.
- **pppoe**—The following PPPoE packet types are available:
  - **padi**—PADI packets.
  - **padm**—PADM packets.
  - **padn**—PADN packets.
  - **pado**—PADO packets.
  - **padr**—PADR packets.
  - **pads**—PADS packets.
  - **padt**—PADT packets.
- **radius**—The following RADIUS packet types are available:
  - **accounting**—RADIUS accounting packets.
  - **authorization**—RADIUS authorization packets.
  - **server**—RADIUS server traffic.
  - **unclassified**—All unclassified packets in the protocol group.

- **tcp-flags**—The following TCP-flagged packet types are available:
  - **established**—TCP ACK and RST connection packets.
  - **initial**—TCP SYN and NAK packets.
- **virtual-chassis**—The following packet types are available for virtual chassis packets:
  - **control-low**—Low-priority control packets.
  - **control-high**—High-priority control packets.
  - **unclassified**—All unclassified packets in the protocol group.
  - **vc-packets**—All exception packets on the virtual chassis link.
  - **vc-ttl-errors**—Virtual chassis TTL error packets.

***protocol-group***—Name of the protocol group for which traffic is policed. You can configure a policer for any of the following protocol groups.

- **anyp**—ANCP traffic.
- **anypv6**—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.
- **firewall-reject**—Packets rejected by a firewall.
- **ftp**—FTP traffic.
- **ftpv6**—FTPv6 traffic.
- **gre**—GRE traffic.
- **icmp**—ICMP traffic.
- **igmp**—IGMP traffic.
- **igmp-snoop**—Control traffic for IGMP snooping.
- **igmpv4v6**—IGMP v4/v6 traffic.
- **igmpv6**—IGMPv6 traffic.
- **ip-fragments**—IP fragments traffic.
- **ip-options**—IP traffic with IP packet header options.

- **ipv4-unclassified**—Unclassified IPv4 host-bound traffic.
- **ipv6-unclassified**—Unclassified IPv6 host-bound traffic.
- **isis**—IS-IS traffic.
- **jfm**—JFM traffic.
- **l2tp**—L2TP traffic.
- **lACP**—LACP traffic.
- **ldp**—LDP traffic.
- **ldpv6**—LDPv6 traffic.
- **lldp**—LLDP traffic.
- **lmp**—LMP traffic.
- **lmpv6**—LMPv6 traffic.
- **mac-host**—Layer 2 MAC send-to-host traffic.
- **mlp**—MLP traffic.
- **msdp**—MSDP traffic.
- **msdpv6**—MSDPv6 traffic.
- **multicast-copy**—Host copy traffic due to multicast routing.
- **mvrp**—MVRP traffic.
- **ntp**—NTP traffic.
- **oam-lfm**—OAM-LFM traffic.
- **ospf**—OSPF traffic.
- **ospfv3v6**—OSPFv3/IPv6 traffic.
- **pfe-alive**—Packet Forwarding Engine keepalive traffic.
- **pim**—PIM traffic.
- **pmvrp**—PMVRP traffic.
- **pos**—POS traffic.
- **ppp**—PPP traffic.
- **pppoe**—PPPoE traffic.
- **ptp**—PTP traffic.
- **pvstp**—PVSTP traffic.
- **radius**—RADIUS traffic.
- **redirect**—Traffic that triggers ICMP redirects.
- **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.

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

## recover-time (DDoS)

---

<b>Syntax</b>	<code>recover-time <i>seconds</i>;</code>
<b>Hierarchy Level</b>	<code>[edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i>)]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	(MX Series routers with Trio MPCs only) Configure how much time must pass since the last detected DDoS violation before the traffic is considered to have recovered from the attack and returned to normal.
<b>Options</b>	<b><i>seconds</i></b> —Period required for the traffic to recover. <b>Range:</b> 1 through 3600 seconds <b>Default:</b> 300
<b>Required Privilege Level</b>	<b>admin</b> —To view this statement in the configuration. <b>admin-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring DDoS Protection Policers for Individual Packet Types on page 10</li></ul>

## traceoptions (DDoS)

---

<b>Syntax</b>	<pre>traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;     level (all   error   info   notice   verbose   warning);     no-remote-trace; }</pre>
<b>Hierarchy Level</b>	[edit system ddos-protection]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Define tracing operations for DDoS processes.
<b>Options</b>	<p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory <code>/var/log</code>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and finally <b>trace-file.2</b>, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"><li>• <b>all</b>—Trace all operations.</li><li>• <b>config</b>—Trace configuration events.</li><li>• <b>events</b>—Trace all events.</li><li>• <b>gres</b>—Trace GRES events.</li><li>• <b>init</b>—Trace daemon initialization.</li><li>• <b>memory</b>—Trace memory management code.</li><li>• <b>protocol</b>—Trace DDoS protocol processing events.</li><li>• <b>rt-sock</b>—Trace routing socket events.</li><li>• <b>signal</b>—Trace signal handling events.</li><li>• <b>state</b>—Trace state machine events.</li><li>• <b>timer</b>—Trace timer events.</li><li>• <b>ui</b>—Trace user interface events.</li></ul>



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

**no-remote-trace**—Disable remote tracing.

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

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

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

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

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

<b>Required Privilege Level</b>	trace—To view this statement in the configuration.
	trace-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Tracing DDoS Protection Operations on page 12</li> </ul>

## violation (DDoS)

<b>Syntax</b>	violation { <b>disable-logging</b> ; }
<b>Hierarchy Level</b>	[edit system ddos-protection protocols <i>protocol-group</i> (aggregate   <i>packet-type</i> ) ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	(MX Series routers with Trio MPCs only) Disable event logging when a DDoS violation occurs; that is, when the configured policer value is exceeded.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration.
	admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring DDoS Protection Policers for Individual Packet Types on page 10</li> </ul>



## PART 2

# Indexes

- Index on page 49
- Index of Statements and Commands on page 51



# Index

## B

bandwidth statement	
DDoS protection.....	29
bandwidth-scale statement	
DDoS protection.....	30
burst statement	
DDoS protection.....	30
burst-scale statement	
DDoS protection.....	31
bypass-aggregate statement	
DDoS protection.....	31

## D

DDoS protection	
configuration example.....	16
configuration overview.....	9
disabling policers and logging globally.....	10
flags for tracing operations.....	14
log file access for tracing operations.....	14
log file size and number.....	13
log filenames.....	13
logging	
disabling globally.....	10
overview.....	3
packet-level configuration.....	10
policers	
aggregate.....	4
disabling globally.....	10
disabling individual.....	10
hierarchy.....	5
packet-level configuration.....	10
protocol.....	4
scaling.....	5
regular expressions for tracing operations.....	14
tracing operations.....	12
traffic priority	
aggregate.....	4
verifying configuration.....	15

## DDoS protection statements

bandwidth.....	29
bandwidth-scale.....	30
burst.....	30
burst-scale.....	31
bypass-aggregate.....	31
ddos-protection.....	32
disable-fpc.....	33
disable-logging.....	33
disable-routing-engine.....	34
fpc.....	34
global.....	35
priority.....	35
protocols.....	36
recover-time.....	43
traceoptions.....	44
violation.....	45
ddos-protection statement	
DDoS protection.....	32
denial-of-service attacks	
protecting against See DDoS Protection	
disable-fpc statement	
DDoS protection.....	33
disable-logging statement	
DDoS protection.....	33
disable-routing-engine statement	
DDoS protection.....	34
distributed denial of service See DDoS protection	

## F

fpc statement	
DDoS protection.....	34

## G

global statement	
DDoS protection.....	35

**L**

log files	
filenames for DDoS protection.....	13
number of DDoS protection.....	13
size of DDoS protection.....	13

**P**

priority statement	
DDoS protection.....	35
protocols statement	
DDoS protection.....	36

**R**

recover-time statement	
DDoS protection.....	43

**T**

tracoptions statement	
DDoS protection.....	44
tracing operations	
DDoS protection.....	12

**V**

violation statement	
DDoS protection.....	45

# Index of Statements and Commands

## B

bandwidth statement	
DDoS protection.....	29
bandwidth-scale statement	
DDoS protection.....	30
burst statement	
DDoS protection.....	30
burst-scale statement	
DDoS protection.....	31
bypass-aggregate statement	
DDoS protection.....	31

## D

DDoS protection statements	
bandwidth.....	29
bandwidth-scale.....	30
burst.....	30
burst-scale.....	31
bypass-aggregate.....	31
ddos-protection.....	32
disable-fpc.....	33
disable-logging.....	33
disable-routing-engine.....	34
fpc.....	34
global.....	35
priority.....	35
protocols.....	36
recover-time.....	43
traceoptions.....	44
violation.....	45
ddos-protection statement	
DDoS protection.....	32
disable-fpc statement	
DDoS protection.....	33
disable-logging statement	
DDoS protection.....	33
disable-routing-engine statement	
DDoS protection.....	34

## F

fpc statement	
DDoS protection.....	34

## G

global statement	
DDoS protection.....	35

## P

priority statement	
DDoS protection.....	35
protocols statement	
DDoS protection.....	36

## R

recover-time statement	
DDoS protection.....	43

## T

traceoptions statement	
DDoS protection.....	44

## V

violation statement	
DDoS protection.....	45

