



JUNOS® Software for EX Series Ethernet Switches, Release 10.0: Device Security

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, California 94089

USA

408-745-2000

www.juniper.net

Revision 1

Published: 2009-11-04

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, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark 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® Software for EX Series Ethernet Switches, Release 10.0: Device Security

Copyright © 2009, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Writing:

Editing:

Illustration:

Cover Design:

Revision History

4 November 2009—Revision 1

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

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)).

Table of Contents

	About This Topic Collection	ix
	How to Use This Guide	ix
	List of EX Series Guides for JUNOS Release 10.0	ix
	Downloading Software	x
	Documentation Symbols Key	xi
	Documentation Feedback	xii
	Requesting Technical Support	xiii
	Self-Help Online Tools and Resources	xiii
	Opening a Case with JTAC	xiii
Part 1	Rate Limiting	
Chapter 1	Rate Limiting	3
	Understanding Storm Control on EX Series Switches	3
	Understanding Unknown Unicast Forwarding on EX Series Switches	4
Chapter 2	Example: Rate Limiting Configuration	5
	Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches	5
Chapter 3	Configuring Rate Limiting	9
	Configuring Unknown Unicast Forwarding (CLI Procedure)	9
	Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)	10
Chapter 4	Verifying Rate Limiting Configuration	11
	Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface	11
	Verifying That the Port Error Disable Setting Is Working Correctly	12

Chapter 5	Configuration Statements for Rate Limiting	13
	[edit ethernet-switching-options] Configuration Statement Hierarchy	13
	action-shutdown	16
	bandwidth	17
	disable-timeout	18
	ethernet-switching-options	19
	interface	22
	interface	23
	no-broadcast	23
	no-unknown-unicast	24
	storm-control	25
	unknown-unicast-forwarding	26
	vlan	27
 Chapter 6	 Operational Mode Commands for Rate Limiting	 29
	show ethernet-switching interfaces	30
	show ethernet-switching table	33

About This Topic Collection

- How to Use This Guide on page ix
- List of EX Series Guides for JUNOS Release 10.0 on page ix
- Downloading Software on page x
- Documentation Symbols Key on page xi
- Documentation Feedback on page xii
- Requesting Technical Support on page xiii

How to Use This Guide

Complete documentation for the EX Series product family is provided on webpages at http://www.juniper.net/techpubs/en_US/release-independent/information-products/pathway-pages/ex-series/product/index.html. We have selected content from these webpages and created a number of EX Series guides that collect related topics into a book-like format so that the information is easy to print and easy to download to your local computer.

The release notes are at http://www.juniper.net/techpubs/en_US/junos10.0/information-products/topic-collections/release-notes/10.0/junos-release-notes-10.0.pdf.

List of EX Series Guides for JUNOS Release 10.0





Title	Description
<i>Complete Hardware Guide for EX3200 and EX4200 Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX3200 and EX4200 switches
<i>Complete Hardware Guide for EX8208 Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8208 switches
<i>Complete Hardware Guide for EX8216 Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8216 switches
<i>Complete Software Guide for JUNOS® Software for EX Series Switches, Release 10.0</i>	Software feature descriptions, configuration examples, and tasks for JUNOS Software for EX Series switches

Title	Description
Software Topic Collections	Software feature descriptions, configuration examples and tasks, and reference pages for configuration statements and operational commands (This information also appears in the <i>Complete Software Guide</i> .)
<i>JUNOS® Software for EX Series Switches, Release 10.0: Access Control</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Alarms and System Log Messages</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Configuration and File Management</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Class of Service</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Device Security</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Ethernet Switching</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Interfaces</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Layer 3 Protocols</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: MPLS</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Multicast</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Network Management and Monitoring</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Port Security</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Routing Policy and Packet Filtering</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Spanning-Tree Protocols</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: System Setup</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: User and Access Management</i>	
<i>JUNOS® Software for EX Series Switches, Release 10.0: Virtual Systems</i>	

Downloading Software

You can download JUNOS Software for EX Series switches from the Download Software area at <http://www.juniper.net/customers/support/>. To download the software, you must have a Juniper Networks user account. For information about obtaining an account, see <http://www.juniper.net/entitlement/setupAccountInfo.do>.

Documentation Symbols Key

Notice Icons		
Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Text and Syntax Conventions		
Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the <code>configure</code> command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> ■ Introduces important new terms. ■ Identifies book names. ■ Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> ■ A policy <i>term</i> is a named structure that defines match conditions and actions. ■ <i>JUNOS System Basics Configuration Guide</i> ■ RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> ■ To configure a stub area, include the <code>stub</code> statement at the [edit protocols ospf area area-id] hierarchy level. ■ The console port is labeled CONSOLE.

Text and Syntax Conventions		
Convention	Description	Examples
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> ■ In the Logical Interfaces box, select All Interfaces. ■ To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select Protocols > Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. Send e-mail to techpubs-comments@juniper.net with the following:

- Document URL or title
- Page number if applicable
- Software version
- Your name and company

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/customers/support/downloads/710059.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

Part 1

Rate Limiting

- Rate Limiting on page 3
- Example: Rate Limiting Configuration on page 5
- Configuring Rate Limiting on page 9
- Verifying Rate Limiting Configuration on page 11
- Configuration Statements for Rate Limiting on page 13
- Operational Mode Commands for Rate Limiting on page 29

Chapter 1

Rate Limiting

- Understanding Storm Control on EX Series Switches on page 3
- Understanding Unknown Unicast Forwarding on EX Series Switches on page 4

Understanding Storm Control on EX Series Switches

A traffic storm is generated when messages are broadcast on a network and each message prompts a receiving node to respond by broadcasting its own messages on the network. This, in turn, prompts further responses, creating a snowball effect. The LAN is suddenly flooded with packets, creating unnecessary traffic that leads to poor network performance or even a complete loss of network service. Storm control enables the switch to monitor traffic levels and drop broadcast and unknown unicast packets when a specified traffic level—called the *storm control level*—is exceeded, thus preventing packets from proliferating and degrading the LAN. Alternatively, you can configure the switch to shut down interfaces (see [action-shutdown](#)) or temporarily disable interfaces (see [port-error-disable](#)) when the storm control level is exceeded.

By default, storm control is enabled on all switch interfaces at a level of 80 percent of the combined broadcast and unknown unicast streams. You can change the storm control level either by configuring it as a bandwidth value for the combined broadcast and unknown unicast traffic streams or by configuring it as a percentage of the combined broadcast and unknown unicast streams.



NOTE: The `level` configuration statement, which allows you to configure the storm control level as a percentage of the combined broadcast and unknown unicast streams, has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use and replace it with the `bandwidth` statement, which allows you to configure the storm control level as a bandwidth value for the combined broadcast and unknown unicast traffic streams.

Broadcast, multicast, and unicast packets are part of normal LAN operation, so to recognize a storm, you must be able to identify when traffic has reached a level that is abnormal for your LAN. Suspect a storm when operations begin timing out and network response times slow down. As more packets flood the LAN, network users might be unable to access servers or e-mail.

Monitor the percentage of broadcast and unknown unicast traffic in the LAN when it is operating normally. This data can then be used as a benchmark to determine

when traffic levels are too high. You can then configure storm control to set the level at which you want to drop broadcast and unknown unicast traffic.

- Related Topics**
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5
 - Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 10

Understanding Unknown Unicast Forwarding on EX Series Switches

Unknown unicast traffic consists of unicast packets with unknown destination MAC addresses. By default, the switch floods these unicast packets that are traveling in a VLAN to all interfaces that are members of the VLAN. Forwarding this type of traffic to interfaces on the switch can trigger a security issue. The LAN is suddenly flooded with packets, creating unnecessary traffic that leads to poor network performance or even a complete loss of network service. This is known as a traffic storm.

To prevent a storm, you can disable the flooding of unknown unicast packets to all interfaces by configuring one VLAN or all VLANs to forward and unknown unicast traffic to a specific trunk interface. This channels the unknown unicast traffic to a single interface.

- Related Topics**
- Understanding Storm Control on EX Series Switches on page 3
 - Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5
 - Configuring Unknown Unicast Forwarding (CLI Procedure) on page 9

Chapter 2

Example: Rate Limiting Configuration

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5

Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches

Storm control enables you to prevent network outages caused by broadcast storms on the LAN. You can configure storm control on the EX Series switch to rate limit broadcast traffic and unknown unicast traffic at a specified level and to drop packets when the specified traffic level is exceeded, thus preventing packets from proliferating and degrading the LAN.

This example shows how to configure storm control on a single EX Series switch:

- Requirements on page 5
- Overview and Topology on page 5
- Configuration of the Storm Control Level Based on the Traffic Rate of the Controlled Traffic Types on page 6
- Configuration of the Storm Control Level Based on a Percentage of the Controlled Traffic Types (Deprecated Method) on page 7

Requirements

This example uses the following hardware and software components:

- One Juniper Networks EX3200 switch
- JUNOS Release 9.1 or later for EX Series switches

Overview and Topology

A storm is generated when messages are broadcast on a network and each message prompts a receiving node to respond by broadcasting its own messages on the network. This, in turn, prompts further responses, creating a snowball effect and resulting in a broadcast storm that can cause network outages.

You can use storm control to prevent broadcast storms by specifying the amount, also known as the storm control level, of broadcast traffic and unknown unicast traffic to be allowed on an interface. This level is given either as the traffic rate in

kilobits per second of the combined broadcast and unknown unicast streams or as a percentage of the combined broadcast and unknown unicast streams.



NOTE: By default, storm control is enabled on all interfaces. The default level is 80 percent of the combined broadcast and unknown unicast streams.

Storm control monitors the incoming broadcast traffic and unknown unicast traffic and compares it with the level that you specify. If broadcast traffic and unknown unicast traffic exceed the specified level, the switch drops packets for the controlled traffic types.



NOTE: Alternatively, you can configure the switch to shut down or temporarily disable the interface when the storm control limit is exceeded. See “Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)” on page 10.

The topology used in this example consists of one EX3200 switch with 24 ports. The switch is connected to various network devices. This example shows how to configure the storm control level on interface `ge-0/0/0` by using one of two different configuration methods:

- Setting the level to a traffic rate of 15000 Kbps, based on the traffic rate of the combined broadcast and unknown unicast streams
- Setting the level to 40 (plus or minus 2) percent, based on the combined broadcast and unknown unicast streams

If broadcast traffic and unknown unicast traffic exceeds these levels, the switch drops packets for the controlled traffic types to prevent a network outage.

Configuration of the Storm Control Level Based on the Traffic Rate of the Controlled Traffic Types

CLI Quick Configuration To quickly configure storm control based on the traffic rate in kilobits per second of the combined broadcast and unknown unicast streams, copy the following command and paste it into the switch terminal window:

```
[edit]
set ethernet-switching-options storm-control interface ge-0/0/0 bandwidth 15000
```

Step-by-Step Procedure To configure storm control based on the traffic rate in kilobits per second of the combined broadcast and unknown unicast streams:

1. Specify the level of allowed broadcast traffic and unknown unicast traffic on a specific interface:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface ge-0/0/0 bandwidth 15000
```

Results Display the results of the configuration:

```
[edit ethernet-switching-options]
user@switch# show storm-control
interface ge-0/0/0.0 {
  bandwidth 15000;
}
```

Configuration of the Storm Control Level Based on a Percentage of the Controlled Traffic Types (Deprecated Method)

CLI Quick Configuration To quickly configure storm control based on the percentage of the combined broadcast and unknown unicast streams, copy the following command and paste it into the switch terminal window:

```
[edit]
set ethernet-switching-options storm-control interface ge-0/0/0 level 40
```



NOTE: The level configuration statement has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use and replace it with the `bandwidth` statement.

Step-by-Step Procedure To configure storm control based on a percentage of the combined broadcast and unknown unicast streams:

1. Specify the level of allowed broadcast traffic and unknown unicast traffic on a specific interface:

```
[edit ethernet-switching-options]
user@switch# set storm-control interface ge-0/0/0 level 40
```



NOTE: The `level` configuration statement has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use and replace it with the `bandwidth` statement.

Results Display the results of the configuration:

```
[edit ethernet-switching-options]
user@switch# show storm-control
interface ge-0/0/0.0 {
  level 40; ## Warning: 'level' is deprecated
}
```

Related Topics ■ [Understanding Storm Control on EX Series Switches on page 3](#)

Chapter 3

Configuring Rate Limiting

- Configuring Unknown Unicast Forwarding (CLI Procedure) on page 9
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 10

Configuring Unknown Unicast Forwarding (CLI Procedure)

Unknown unicast traffic consists of packets with unknown destination MAC addresses. By default, the switch floods these packets to all interfaces associated with a VLAN. Forwarding such traffic to interfaces on the switch can create a security issue.

To prevent flooding unknown unicast traffic across the switch, configure unknown unicast forwarding to direct all unknown unicast packets within a VLAN out to a specific trunk interface. From there, the destination MAC address can be learned and added to the Ethernet switching table. You can configure each VLAN to divert unknown unicast traffic to different trunk interfaces or use one trunk interface for multiple VLANs.

To configure unknown unicast forwarding options using the CLI:



NOTE: Before you can configure unknown unicast forwarding within a VLAN, you must first configure that VLAN.

1. Configure unknown unicast forwarding for a specific VLAN (here, the VLAN name is `employee`):

```
[edit ethernet-switching-options]
user@switch# set unknown-unicast-forwarding vlan employee
```

2. Specify the trunk interface to which all unknown unicast traffic will be forwarded:

```
[edit ethernet-switching-options ]
user@switch# set unknown-unicast-forwarding vlan employee interface ge-0/0/3.0
```

- Related Topics**
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5
 - Configuring VLANs for EX Series Switches (CLI Procedure)

- Configuring VLANs for EX Series Switches (J-Web Procedure)
- Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface on page 11
- Understanding Unknown Unicast Forwarding on EX Series Switches on page 4
- Understanding Storm Control on EX Series Switches on page 3

Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)

An Ethernet switching access interface on an EX Series switch might shut down or be disabled as a result of one of the following port-security or storm-control configurations:

- MAC limiting—`mac-limit` statement is configured with action `shutdown`.
- MAC move limiting—`mac-move-limit` statement is configured with action `shutdown`.
- Storm control—`storm-control` statement is configured with the action `shutdown`.

You can configure the switch to automatically restore the disabled interfaces to service after a specified period of time. Autorecovery applies to all the interfaces that have been disabled due to MAC limiting, MAC move limiting, or storm control errors.



NOTE: You must specify the disable timeout value for the interfaces to recover automatically. There is no default disable timeout. If you do not specify a timeout value, you need to use the `clear ethernet-switching port-error` command to clear the errors and restore the interfaces or the specified interface to service.

To configure autorecovery from the disabled state due to MAC limiting, MAC move limiting, or storm control shutdown actions:

```
[edit ethernet-switching-options]
user@switch# set port-error-disable disable-timeout 60
```

- Related Topics**
- Example: Configuring Port Security, with DHCP Snooping, DAI, MAC Limiting, and MAC Move Limiting, on an EX Series Switch
 - Configuring MAC Limiting (CLI Procedure)
 - Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5
 - Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches
 - Understanding Storm Control on EX Series Switches on page 3

Chapter 4

Verifying Rate Limiting Configuration

- Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface on page 11
- Verifying That the Port Error Disable Setting Is Working Correctly on page 12

Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface

Purpose Verify that a VLAN is forwarding all unknown unicast packets (those with unknown destination MAC addresses) to a single trunk interface instead of flooding unknown unicast packets across all interfaces that are members of the same VLAN.

Action Display the forwarding interface for unknown unicast packets for a VLAN (here, the VLAN name is v1):

```
user@switch> show configuration ethernet-switching-options

unknown-unicast-forwarding {
    vlan v1 {
        interface ge-0/0/7.0;
    }
}
```

Display the Ethernet switching table:

```
user@switch> show ethernet-switching table vlan v1
Ethernet-switching table: 3 unicast entries
VLAN      MAC address      Type      Age Interfaces
v1        *                 Flood     - All-members
v1        00:01:09:00:00:00 Learn     24 ge-0/0/7.0
v1        00:11:09:00:01:00 Learn     37 ge-0/0/3.0
```

Meaning The sample output from the `show configuration ethernet-switching-options` command shows that the unknown unicast forwarding interface for VLAN v1 is interface ge-0/0/7. The `show ethernet-switching table` command shows that an unknown unicast packet is received on interface ge-0/0/3 with the destination MAC address (DMAC) 00:01:09:00:00:00 and the source MAC address (SMAC) of 00:11:09:00:01:00. This shows that the SMAC of the packet is learned in the normal way (through the interface ge-0/0/3.0), while the DMAC is learned on interface ge-0/0/7.

Related Topics ■ Configuring Unknown Unicast Forwarding (CLI Procedure) on page 9

Verifying That the Port Error Disable Setting Is Working Correctly

Purpose Verify that the port error disable setting is working as expected on MAC limited, MAC move limited and rate-limited interfaces on an EX Series switch.

Action Display information about interfaces:

```
user@switch> show ethernet-switching interfaces
Interface  State  VLAN members  Blocking
ge-0/0/0.0  up    T1122         unblocked
ge-0/0/1.0  down  default      MAC limit exceeded
ge-0/0/2.0  down  default      MAC move limit exceeded
ge-0/0/3.0  down  default      Storm control in effect
ge-0/0/4.0  down  default      unblocked
ge-0/0/5.0  down  default      unblocked
ge-0/0/6.0  down  default      unblocked
ge-0/0/7.0  down  default      unblocked
ge-0/0/8.0  down  default      unblocked
ge-0/0/9.0  up    T111         unblocked
ge-0/0/10.0 down  default      unblocked
ge-0/0/11.0 down  default      unblocked
ge-0/0/12.0 down  default      unblocked
ge-0/0/13.0 down  default      unblocked
ge-0/0/14.0 down  default      unblocked
ge-0/0/15.0 down  default      unblocked
ge-0/0/16.0 down  default      unblocked
ge-0/0/17.0 down  default      unblocked
ge-0/0/18.0 down  default      unblocked
ge-0/0/19.0 up    T111         unblocked
ge-0/1/0.0  down  default      unblocked
ge-0/1/1.0  down  default      unblocked
ge-0/1/2.0  down  default      unblocked
ge-0/1/3.0  down  default      unblocked
```

Meaning The sample output from the `show ethernet-switching interfaces` command shows that three of the down interfaces specify the reason that the interface is disabled:

- **MAC limit exceeded**—The interface is temporarily disabled due to a mac-limit error. The disabled interface is automatically restored to service when the `disable-timeout` expires.
- **MAC move limit exceeded**—The interface is temporarily disabled due to a mac-move-limit error. The disabled interface is automatically restored to service when the `disable-timeout` expires.
- **Storm control in effect** —The interface is temporarily disabled due to a storm-control error. The disabled interface is automatically restored to service when the `disable-timeout` expires.

Related Topics ■ Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 10

Chapter 5

Configuration Statements for Rate Limiting

- [edit ethernet-switching-options] Configuration Statement Hierarchy on page 13

[edit ethernet-switching-options] Configuration Statement Hierarchy

```
ethernet-switching-options {
  analyzer {
    name {
      loss-priority priority;
      ratio number;
      input {
        ingress {
          interface (all | interface-name);
          vlan (vlan-id | vlan-name);
        }
        egress {
          interface (all | interface-name);
        }
      }
      output {
        interface interface-name;
        vlan (vlan-id | vlan-name);
      }
    }
  }
  bpdu-block {
    disable-timeout timeout;
    interface (all | [interface-name]);
  }
  dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100) ;
  }
  interfaces interface-name {
    no-mac-learning;
  }
  mac-table-aging-time seconds;
  port-error-disable {
    disable-timeout timeout;
  }
  redundant-trunk-group {
    group-name name {
      interface interface-name <primary>;
    }
  }
}
```

```

    }
  }
  secure-access-port {
    dhcp-snooping-file {
      location local_pathname | remote_URL;
      timeout seconds;
      write-interval seconds;
    }
    interface (all | interface-name) {
      allowed-mac {
        mac-address-list;
      }
      (dhcp-trusted | no-dhcp-trusted );
      mac-limit limit action action;
      no-allowed-mac-log;
      static-ip ip-address {
        vlan vlan-name;
        mac mac-address;
      }
    }
  }
  vlan (all | vlan-name) {
    (arp-inspection | no-arp-inspection );
    dhcp-option82 {
      circuit-id {
        prefix hostname;
        use-interface-description;
        use-vlan-id;
      }
      remote-id {
        prefix hostname | mac | none;
        use-interface-description;
        use-string string;
      }
      vendor-id [string];
    }
    (examine-dhcp | no-examine-dhcp );
    (ip-source-guard | no-ip-source-guard);
    mac-move-limit limit action action;
  }
}
storm-control {
  interface (all | interface-name) {
    bandwidth bandwidth;
    no-broadcast;
    no-unknown-unicast;
  }
}
traceoptions {
  file filename <files number> <no-stamp> <replace> <size size> <world-readable
  | no-world-readable>;
  flag flag <disable>;
}
unknown-unicast-forwarding {
  vlan (all | vlan-name) {
    interface interface-name;
  }
}

```

```

}
voip {
  interface (all | [interface-name | access-ports]) {
    vlan vlan-name ;
    forwarding-class <assured-forwarding | best-effort | expedited-forwarding |
    network-control>;
  }
}
}

```

- Related Topics**
- Understanding Port Mirroring on EX Series Switches
 - Port Security for EX Series Switches Overview
 - Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches
 - Understanding Redundant Trunk Links on EX Series Switches
 - Understanding Storm Control on EX Series Switches on page 3
 - Understanding 802.1X and VoIP on EX Series Switches
 - Understanding Q-in-Q Tunneling on EX Series Switches
 - Understanding Unknown Unicast Forwarding on EX Series Switches on page 4

action-shutdown

Syntax	action-shutdown;
Hierarchy Level	[edit ethernet-switching-options storm-control]
Release Information	Statement introduced in JUNOS Release 9.6 for EX Series switches.
Description	<p>Shut down or disable interfaces when the storm control level is exceeded, as follows:</p> <ul style="list-style-type: none"> ■ If you set both the action-shutdown and the port-error-disable statements, the interfaces are disabled temporarily and recover automatically when the disable timeout expires. ■ If you set the action-shutdown statement and do not specify the port-error-disable statement, the interfaces that are enabled for storm control are shut down when the storm control level is exceeded and they do not recover automatically from that port-error condition. You must issue the clear ethernet-switching port-error command to clear the port error and restore the interfaces to service.
Default	The action-shutdown option is not enabled. When the storm control level is exceeded, the switch drops unknown unicast and broadcast messages on the specified interfaces.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ port-error-disable ■ disable-timeout ■ clear ethernet-switching port-error ■ Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5 ■ Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 10 ■ Understanding Storm Control on EX Series Switches on page 3

bandwidth

Syntax	bandwidth <i>bandwidth</i> ;
Hierarchy Level	[edit ethernet-switching-options storm-control interface (all <i>interface-name</i>)]
Release Information	Statement introduced in JUNOS Release 9.5 for EX Series switches.
Description	For interfaces configured for storm control, configure the storm control level as the bandwidth in kilobits per second of the combined broadcast and unknown unicast streams.
Default	None.
Options	<p>bandwidth—Traffic rate in kilobits per second of the combined broadcast and unknown unicast streams.</p> <p>Range: 100 through 10000000 Kbps</p> <p>Default: None</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5 ■ Understanding Storm Control on EX Series Switches on page 3

disable-timeout

Syntax	disable-timeout <i>timeout</i> ;
Hierarchy Level	[edit ethernet-switching-options port-error-disable]
Release Information	Statement introduced in JUNOS Release 9.6 for EX Series switches.
Description	Specify how long the Ethernet-switching interfaces remain in a disabled state due to the MAC limiting, MAC move limiting, or storm control errors.
Default	The disable timeout is not enabled.
Options	<i>timeout</i> —Amount of time, in seconds, that the disabled state remains in effect. The disabled interface is automatically restored to service when the specified timeout is reached. Range: 10 through 3600 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none">■ Configuring Port Security (CLI Procedure)■ Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 10■ Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5

ethernet-switching-options

```

Syntax ethernet-switching-options {
    analyzer {
        name {
            loss-priority priority;
            ratio number;
            input {
                ingress {
                    interface (all | interface-name);
                    vlan (vlan-id | vlan-name);
                }
                egress {
                    interface (all | interface-name);
                }
            }
            output {
                interface interface-name;
                vlan (vlan-id | vlan-name);
            }
        }
    }
    bpdu-block {
        disable-timeout timeout;
        interface (all | [interface-name]);
    }
    dot1q-tunneling {
        ether-type (0x8100 | 0x88a8 | 0x9100)
    }
    interfaces interface-name {
        no-mac-learning;
    }
    mac-table-aging-time seconds;
    port-error-disable {
        disable-timeout timeout;
    }
    redundant-trunk-group {
        group-name name {
            interface interface-name <primary>;
            interface interface-name;
        }
    }
    secure-access-port {
        dhcp-snooping-file {
            location local_pathname | remote_URL;
            timeout seconds;
            write-interval seconds;
        }
        interface (all | interface-name) {
            allowed-mac {
                mac-address-list;
            }
            (dhcp-trusted | no-dhcp-trusted);
            mac-limit limit action action;
        }
    }
}

```

```

        no-allowed-mac-log;
        static-ip ip-address {
            vlan vlan-name;
            mac mac-address;
        }
    }
    vlan (all | vlan-name) {
        (arp-inspection | no-arp-inspection);
        dhcp-option82 {
            circuit-id {
                prefix hostname;
                use-interface-description;
                use-vlan-id;
            }
            remote-id {
                prefix hostname | mac | none;
                use-interface-description;
                use-string string;
            }
            vendor-id [string];
        }
        (examine-dhcp | no-examine-dhcp);
        (ip-source-guard | no-ip-source-guard);
        mac-move-limit limit action action;
    }
}
storm-control {
    interface (all | interface-name) {
        level level;
        no-broadcast;
        no-unknown-unicast;
    }
}
traceoptions {
    file filename <files number> <no-stamp> <replace> <size size> <world-readable |
    no-world-readable>;
    flag flag <disable>;
}
unknown-unicast-forwarding {
    vlan (all | vlan-name) {
        interface interface-name;
    }
}
voip {
    interface (all | [interface-name | access-ports]) {
        vlan vlan-name ;
        forwarding-class <assured-forwarding | best-effort | expedited-forwarding |
        network-control>;
    }
}
}

```

Hierarchy Level [edit]

Release Information Statement introduced in JUNOS Release 9.0 for EX Series switches.
 Support for storm control and BPDU protection added in JUNOS Release 9.1 for EX Series switches.
 Option `ip-source-guard` added in JUNOS Release 9.2 for EX Series switches.
 Options `dhcp-option82`, `dot1q-tunneling`, and `no-allowed-mac-log` added in JUNOS Release 9.3 for EX Series switches.
 Options `dhcp-snooping-file` and `mac-table-aging-time` introduced in JUNOS Release 9.4 for EX Series switches.
 Options `interfaces` and `no-mac-learning` introduced in JUNOS Release 9.5 for EX Series switches.
 Options `port-error-disable` and `disable-timeout` introduced in JUNOS Release 9.6 for EX Series switches.

Description Configure Ethernet switching options.

The remaining statements are explained separately.

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

Related Topics

- Understanding Port Mirroring on EX Series Switches
- Port Security for EX Series Switches Overview
- Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches
- Understanding Redundant Trunk Links on EX Series Switches
- Understanding Storm Control on EX Series Switches on page 3
- Understanding 802.1X and VoIP on EX Series Switches
- Understanding Q-in-Q Tunneling on EX Series Switches
- Understanding Unknown Unicast Forwarding on EX Series Switches on page 4

interface

Syntax interface (all | *interface-name*) {
 bandwidth *bandwidth*;
 no-broadcast;
 no-unknown-unicast;
 }

Hierarchy Level [edit ethernet-switching-options storm-control]

Release Information Statement introduced in JUNOS Release 9.1 for EX Series switches.

Description Apply storm control to all interfaces or to the specified interface.

The statements are explained separately.

Default Storm control is enabled on all switch interfaces at a level of 80 percent of the combined broadcast and unknown unicast streams.

Options all—Apply storm control to all interfaces.

interface-name—Apply storm control to the specified interface.

The remaining statements are explained separately.


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

- Related Topics**
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5
 - Understanding Storm Control on EX Series Switches on page 3

interface

Syntax	<code>interface interface-name;</code>
Hierarchy Level	[edit ethernet-switching-options unknown-unicast-forwarding vlan(all vlan-name)]
Release Information	Statement introduced in JUNOS Release 9.3 for EX Series switches.
Description	Specify the interface to which unknown unicast packets will be forwarded.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ show vlans ■ show ethernet-switching table ■ Configuring Unknown Unicast Forwarding (CLI Procedure) on page 9 ■ Understanding Unknown Unicast Forwarding on EX Series Switches on page 4

no-broadcast

Syntax	<code>no-broadcast;</code>
Hierarchy Level	[edit ethernet-switching-options storm-control interface (all interface-name)]
Release Information	Statement introduced in JUNOS Release 9.1 for EX Series switches. Statement deprecated in JUNOS Release 9.4 for EX Series switches.
	NOTE: If you configure this statement, it has no effect. This statement has been deprecated and might be removed from future product releases.
Description	For interfaces configured for storm control, disable broadcast traffic storm control on the interface.
Default	When storm control is enabled on an interface, it is enabled for both unknown unicast traffic and broadcast traffic.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5 ■ Understanding Storm Control on EX Series Switches on page 3

no-unknown-unicast

Syntax no-unknown-unicast;

Hierarchy Level [edit ethernet-switching-options storm-control interface (all | *interface-name*)]

Release Information Statement introduced in JUNOS Release 9.1 for EX Series switches.
Statement deprecated in JUNOS Release 9.4 for EX Series switches.



NOTE: If you configure this statement, it has no effect. This statement has been deprecated and might be removed from future product releases.

Description For interfaces configured for storm control, disable unknown unicast traffic storm control on the interface.

Default When storm control is enabled on an interface, it is enabled for both unknown unicast traffic and broadcast traffic.

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

Related Topics

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5
- Understanding Storm Control on EX Series Switches on page 3

storm-control

Syntax

```
storm-control {
  action-shutdown;
  interface (all | interface-name) {
    bandwidth bandwidth;
    no-broadcast;
    no-unknown-unicast;
  }
}
```

Hierarchy Level [edit ethernet-switching-options]

Release Information Statement introduced in JUNOS Release 9.1 for EX Series switches.
Option `action-shutdown` introduced in JUNOS Release 9.6 for EX Series switches.

Description Apply storm control to all interfaces or to the specified interfaces.

The statements are explained separately.

Default By default, storm control is enabled on all switch interfaces at a level of 80 percent of the combined broadcast and unknown unicast streams. You can change the storm control level either by configuring it as a bandwidth value for the combined broadcast and unknown unicast traffic streams or by configuring it as a percentage of the combined broadcast and unknown unicast streams.

When you configure storm control bandwidth on an aggregated Ethernet interface, each member of the aggregated Ethernet interface is set with that bandwidth. For example, if you configure 15000 Kbps on `ae1`, and `ae1` has two members, `ge-0/0/0` and `ge-0/0/1`, each member is allowed a bandwidth level of 15000 Kbps. Thus, the storm control bandwidth on `ae1` could be up to 30000 Kbps of combined broadcast and unknown unicast traffic streams.

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

- Related Topics**
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5
 - Understanding Storm Control on EX Series Switches on page 3

unknown-unicast-forwarding

Syntax unknown-unicast-forwarding {
 vlan (all | *vlan-name*){
 interface *interface-name*;
 }
 }

Hierarchy Level [edit ethernet-switching-options]

Release Information Statement introduced in JUNOS Release 9.3 for EX Series switches.

Description Configure the switch to forward all unknown unicast packets in a VLAN or on all VLANs to a particular interface.



NOTE: Before you can configure unknown unicast forwarding within a VLAN, you must first configure that VLAN.

The remaining statements are explained separately.

Default Unknown unicast packets are flooded to all interfaces that belong to the same VLAN.

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

- Related Topics**
- show vlans
 - show ethernet-switching table
 - Configuring Unknown Unicast Forwarding (CLI Procedure) on page 9
 - Understanding Unknown Unicast Forwarding on EX Series Switches on page 4

vlan

Syntax `vlan (all | vlan-name) {
 interface interface-name;
}`

Hierarchy Level [edit ethernet-switching-options unknown-unicast-forwarding]

Release Information Statement introduced in JUNOS Release 9.3 for EX Series switches. Statement updated with enhanced ? (CLI completion feature) functionality in JUNOS Release 9.5 for EX Series switches.

Description Specify a VLAN from which unknown unicast packets will be forwarded or specify that the packets will be forwarded from all VLANs. Unknown unicast packets are forwarded from a VLAN to a specific trunk interface.

The `interface` statement is explained separately.



TIP: To display a list of all configured VLANs on the system, including VLANs that are configured but not committed, type ? after `vlan` or `vlangs` in your configuration mode command line. Note that only one VLAN is displayed for a VLAN range.

Options `all`—All VLANs.

`vlan-name`—Name of a VLAN.

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

- Related Topics**
- `show vlans`
 - `show ethernet-switching table`
 - Configuring Unknown Unicast Forwarding (CLI Procedure) on page 9
 - Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface on page 11
 - Understanding Unknown Unicast Forwarding on EX Series Switches on page 4

Chapter 6

Operational Mode Commands for Rate Limiting

show ethernet-switching interfaces

- Syntax** show ethernet-switching interfaces
 <brief | detail | summary>
 <interface *interface-name*>
- Release Information** Command introduced in JUNOS Release 9.0 for EX Series switches. In JUNOS Release 9.6 for EX Series switches, the following updates were made:
- Blocking field output updated.
 - The default view updated to include information about 802.1Q-tags.
 - The detail view updated to include information VLAN mapping.
- Description** Display information about switched Ethernet interfaces.
- Options** none—(Optional) Display brief information for Ethernet switching interfaces.
- brief | detail | summary—(Optional) Display the specified level of output.
- interface *interface-name*—(Optional) Display Ethernet switching information for a specific interface.
- Required Privilege Level** view
- Related Topics**
- show ethernet-switching mac-learning-log
 - show ethernet-switching table
 - Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 10
- List of Sample Output**
- show ethernet-switching interfaces on page 31
 - show ethernet-switching interfaces ge-0/0/15 brief on page 32
 - show ethernet-switching interfaces ge-0/0/2 detail (Blocked by RTG rtggroup) on page 32
 - show ethernet-switching interfaces ge-0/0/15 detail (Blocked by STP) on page 32
 - show ethernet-switching interfaces ge-0/0/17 detail (Disabled by bpdu-control) on page 32
 - show ethernet-switching interfaces detail (C-VLAN to S-VLAN Mapping) on page 32
- Output Fields** Table 1 on page 30 lists the output fields for the show ethernet-switching interfaces command. Output fields are listed in the approximate order in which they appear.

Table 1: show ethernet-switching interfaces Output Fields

Field Name	Field Description	Level of Output
Interface	Name of a switching interface.	All levels
State	Interface state. Values are up and down.	none, brief, detail, summary

Table 1: show ethernet-switching interfaces Output Fields (continued)

Field Name	Field Description	Level of Output
VLAN members	Name of a VLAN.	none, brief, detail, summary
Tag	Number of the 802.1Q-tag.	All levels
Tagging	Specifies whether the interface forwards 802.1Q-tagged or untagged traffic.	All levels
Blocking	The forwarding state of the interface: <ul style="list-style-type: none"> ■ unblocked—Traffic is forwarded on the interface. ■ blocked—Traffic is not being forwarded on the interface. ■ Disabled by bpd control—The interface is disabled due to receiving BPDUs on a protected interface. If the <code>disable-timeout</code> statement has been included in the BPDU configuration, the interface automatically returns to service after the timer expires. ■ blocked by RTG—The specified redundant trunk group is disabled. ■ blocked by STP—The interface is disabled due to a spanning tree protocol error. ■ MAC limit exceeded—The interface is temporarily disabled due to a MAC limiting error. The disabled interface is automatically restored to service when the disable timeout expires. ■ MAC move limit exceeded—The interface is temporarily disabled due to a MAC move limiting error. The disabled interface is automatically restored to service when the disable timeout expires. ■ Storm control in effect—The interface is temporarily disabled due to a storm control error. The disabled interface is automatically restored to service when the disable timeout expires. 	none, brief, detail, summary
Index	The VLAN index internal to JUNOS Software.	detail
mapping	The C-VLAN to S-VLAN mapping information: <ul style="list-style-type: none"> ■ dot1q-tunneled—The interface maps all traffic to the S-VLAN (all-in-one bundling). ■ native—The interface maps untagged and priority tagged packets to the S-VLAN. ■ push—The interface maps packets to a firewall filter to an S-VLAN. ■ policy-mapped—The interface maps packets to a specifically defined S-VLAN. ■ integer—The interface maps packets to the specified S-VLAN. 	detail

show ethernet-switching interfacesuser@switch> **show ethernet-switching interfaces**

```

Interface   State  VLAN members      Tag  Tagging  Blocking
-----
ae0.0      up     default           300  untagged unblocked
ge-0/0/2.0 up     vlan300          300  untagged blocked by RTG (rtggroup)
ge-0/0/3.0 up     default           300  untagged blocked by STP
ge-0/0/4.0 down   default           300  untagged MAC limit exceeded
ge-0/0/5.0 down   default           300  untagged MAC move limit exceeded
ge-0/0/6.0 down   default           300  untagged Storm control in effect

```

```

ge-0/0/7.0 down default unblocked
ge-0/0/13.0 up default untagged unblocked
ge-0/0/14.0 up vlan100 100 tagged unblocked
                vlan200 200 tagged unblocked
ge-0/0/15.0 up vlan100 100 tagged blocked by STP
                vlan200 200 tagged blocked by STP
ge-0/0/16.0 down default untagged unblocked
ge-0/0/17.0 down vlan100 100 tagged Disabled by bpdu-control
                vlan200 200 tagged Disabled by bpdu-control

```

```

show ethernet-switching user@switch> show ethernet-switching interfaces ge-0/0/15 brief
interfaces ge-0/0/15 Interface State VLAN members Tag Tagging Blocking
brief
ge-0/0/15.0 up vlan100 100 tagged blocked by STP
                vlan200 200 tagged blocked by STP

```

```

show ethernet-switching user@switch> show ethernet-switching interfaces ge-0/0/2 detail
interfaces ge-0/0/2 Interface: ge-0/0/2.0, Index: 65, State: up, Port mode: Access
detail (Blocked by RTG VLAN membership:
rtggroup)      vlan300, 802.1Q Tag: 300, untagged, msti-id: 0, blocked by RTG(rtggroup)
Number of MACs learned on IFL: 0

```

```

show ethernet-switching user@switch> show ethernet-switching interfaces ge-0/0/15 detail
interfaces ge-0/0/15 Interface: ge-0/0/15.0, Index: 70, State: up, Port mode: Trunk
detail (Blocked by STP) VLAN membership:
                        vlan100, 802.1Q Tag: 100, tagged, msti-id: 0, blocked by STP
                        vlan200, 802.1Q Tag: 200, tagged, msti-id: 0, blocked by STP
Number of MACs learned on IFL: 0

```

```

show ethernet-switching user@switch> show ethernet-switching interfaces ge-0/0/17 detail
interfaces ge-0/0/17 Interface: ge-0/0/17.0, Index: 71, State: down, Port mode: Trunk
detail (Disabled by VLAN membership:
bpdu-control)      vlan100, 802.1Q Tag: 100, tagged, msti-id: 1, Disabled by bpdu-control
                        vlan200, 802.1Q Tag: 200, tagged, msti-id: 2, Disabled by bpdu-control
Number of MACs learned on IFL: 0

```

```

show ethernet-switching user@switch> show ethernet-switching interfaces ge-0/0/6.0 detail
interfaces detail Interface: ge-0/0/6.0, Index: 73, State: up, Port mode: Access
(C-VLAN to S-VLAN VLAN membership:
Mapping)      map, 802.1Q Tag: 134, Mapped Tag: native, push, dot1q-tunneled, unblocked
                        map, 802.1Q Tag: 134, Mapped Tag: 20, push, dot1q-tunneled, unblocked

```

show ethernet-switching table

Syntax	show ethernet-switching table <brief detail extensive summary> <interface <i>interface-name</i> > <management-vlan> <vlan (<i>vlan-name</i>)>
Release Information	Command introduced in JUNOS Release 9.0 for EX Series switches. Options <i>summary</i> , <i>management-vlan</i> , and <i>vlan vlan-name</i> introduced in JUNOS Release 9.6 for EX Series switches.
Description	Displays the Ethernet switching table.
Options	<p><i>none</i>—(Optional) Display brief information about the Ethernet switching table.</p> <p><i>brief detail extensive summary</i>—(Optional) Display the specified level of output.</p> <p><i>management-vlan</i>—(Optional) Display the Ethernet switching table for a management VLAN.</p> <p><i>interface-name</i>—(Optional) Display the Ethernet switching table for a specific interface.</p> <p><i>vlan vlan-name</i>—(Optional) Display the Ethernet switching table for a specific VLAN.</p>
Required Privilege Level	view
Related Topics	<ul style="list-style-type: none"> ■ Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch ■ Example: Setting Up Bridging with Multiple VLANs for EX Series Switches ■ Example: Configure Automatic VLAN Administration Using GVRP ■ Example: Setting Up Q-in-Q Tunneling on EX Series Switches
List of Sample Output	<p>show ethernet-switching table on page 34</p> <p>show ethernet-switching table brief on page 34</p> <p>show ethernet-switching table detail on page 35</p> <p>show ethernet-switching table extensive on page 36</p> <p>show ethernet-switching table interface ge-0/0/1 on page 38</p>
Output Fields	Table 2 on page 33 lists the output fields for the <code>show ethernet-switching table</code> command. Output fields are listed in the approximate order in which they appear.

Table 2: show ethernet-switching table Output Fields

Field Name	Field Description	Level of Output
VLAN	The name of a VLAN.	All levels
MAC address	The MAC address associated with the VLAN.	All levels

Table 2: show ethernet-switching table Output Fields (continued)

Field Name	Field Description	Level of Output
Type	The type of MAC address. Values are: <ul style="list-style-type: none"> ■ static—The MAC address is manually created. ■ learn—The MAC address is learned dynamically from a packet's source MAC address. ■ flood—The MAC address is unknown and flooded to all members. 	All levels
Age	The time remaining before the entry ages out and is removed from the Ethernet switching table.	All levels
Interfaces	Interface associated with learned MAC addresses or All-members (flood entry).	All levels
Learned	For learned entries, the time which the entry was added to the Ethernet-switching table.	detail, extensive

```

show ethernet-switching table user@switch> show ethernet-switching table
Ethernet-switching table: 57 entries, 17 learned
VLAN      MAC address      Type      Age Interfaces
F2         *                Flood     - All-members
F2         00:00:05:00:00:03 Learn     0 ge-0/0/44.0
F2         00:19:e2:50:7d:e0 Static    - Router
Linux      *                Flood     - All-members
Linux      00:19:e2:50:7d:e0 Static    - Router
Linux      00:30:48:90:54:89 Learn     0 ge-0/0/47.0
T1         *                Flood     - All-members
T1         00:00:05:00:00:01 Learn     0 ge-0/0/46.0
T1         00:00:5e:00:01:00 Static    - Router
T1         00:19:e2:50:63:e0 Learn     0 ge-0/0/46.0
T1         00:19:e2:50:7d:e0 Static    - Router
T10        *                Flood     - All-members
T10        00:00:5e:00:01:09 Static    - Router
T10        00:19:e2:50:63:e0 Learn     0 ge-0/0/46.0
T10        00:19:e2:50:7d:e0 Static    - Router
T111       *                Flood     - All-members
T111       00:19:e2:50:63:e0 Learn     0 ge-0/0/15.0
T111       00:19:e2:50:7d:e0 Static    - Router
T111       00:19:e2:50:ac:00 Learn     0 ge-0/0/15.0
T2         *                Flood     - All-members
T2         00:00:5e:00:01:01 Static    - Router
T2         00:19:e2:50:63:e0 Learn     0 ge-0/0/46.0
T2         00:19:e2:50:7d:e0 Static    - Router
T3         *                Flood     - All-members
T3         00:00:5e:00:01:02 Static    - Router
T3         00:19:e2:50:63:e0 Learn     0 ge-0/0/46.0
T3         00:19:e2:50:7d:e0 Static    - Router
T4         *                Flood     - All-members
T4         00:00:5e:00:01:03 Static    - Router
T4         00:19:e2:50:63:e0 Learn     0 ge-0/0/46.0
[output truncated]
    
```

```

show ethernet-switching table brief user@switch> show ethernet-switching table brief
Ethernet-switching table: 57 entries, 17 learned
VLAN      MAC address      Type      Age Interfaces
F2         *                Flood     - All-members
    
```

```

F2          00:00:05:00:00:03 Learn      0 ge-0/0/44.0
F2          00:19:e2:50:7d:e0 Static     - Router
Linux       *                Flood     - All-members
Linux       00:19:e2:50:7d:e0 Static     - Router
Linux       00:30:48:90:54:89 Learn      0 ge-0/0/47.0
T1          *                Flood     - All-members
T1          00:00:05:00:00:01 Learn      0 ge-0/0/46.0
T1          00:00:5e:00:01:00 Static     - Router
T1          00:19:e2:50:63:e0 Learn      0 ge-0/0/46.0
T1          00:19:e2:50:7d:e0 Static     - Router
T10         *                Flood     - All-members
T10         00:00:5e:00:01:09 Static     - Router
T10         00:19:e2:50:63:e0 Learn      0 ge-0/0/46.0
T10         00:19:e2:50:7d:e0 Static     - Router
T111        *                Flood     - All-members
T111        00:19:e2:50:63:e0 Learn      0 ge-0/0/15.0
T111        00:19:e2:50:7d:e0 Static     - Router
T111        00:19:e2:50:ac:00 Learn      0 ge-0/0/15.0
T2          *                Flood     - All-members
T2          00:00:5e:00:01:01 Static     - Router
T2          00:19:e2:50:63:e0 Learn      0 ge-0/0/46.0
T2          00:19:e2:50:7d:e0 Static     - Router
T3          *                Flood     - All-members
T3          00:00:5e:00:01:02 Static     - Router
T3          00:19:e2:50:63:e0 Learn      0 ge-0/0/46.0
T3          00:19:e2:50:7d:e0 Static     - Router
T4          *                Flood     - All-members
T4          00:00:5e:00:01:03 Static     - Router
T4          00:19:e2:50:63:e0 Learn      0 ge-0/0/46.0

```

[output truncated]

show ethernet-switching table detail

```

user@switch> show ethernet-switching table detail
Ethernet-switching table: 57 entries, 17 learned

```

```

F2, *
  Interface(s): ge-0/0/44.0
  Type: Flood
  Nexthop index: 0

F2, 00:00:05:00:00:03
  Interface(s): ge-0/0/44.0
  Type: Learn, Age: 0, Learned: 2:03:09
  Nexthop index: 0

F2, 00:19:e2:50:7d:e0
  Interface(s): Router
  Type: Static
  Nexthop index: 0

Linux, *
  Interface(s): ge-0/0/47.0
  Type: Flood
  Nexthop index: 0

Linux, 00:19:e2:50:7d:e0
  Interface(s): Router
  Type: Static
  Nexthop index: 0

Linux, 00:30:48:90:54:89
  Interface(s): ge-0/0/47.0
  Type: Learn, Age: 0, Learned: 2:03:08

```

```

    Nexthop index: 0

T1, *
  Interface(s): ge-0/0/46.0
  Type: Flood
  Nexthop index: 0

T1, 00:00:05:00:00:01
  Interface(s): ge-0/0/46.0
  Type: Learn, Age: 0, Learned: 2:03:07
  Nexthop index: 0

T1, 00:00:5e:00:01:00
  Interface(s): Router
  Type: Static
  Nexthop index: 0

T1, 00:19:e2:50:63:e0
  Interface(s): ge-0/0/46.0
  Type: Learn, Age: 0, Learned: 2:03:07
  Nexthop index: 0

T1, 00:19:e2:50:7d:e0
  Interface(s): Router
  Type: Static
  Nexthop index: 0

T10, *
  Interface(s): ge-0/0/46.0
  Type: Flood
  Nexthop index: 0

T10, 00:00:5e:00:01:09
  Interface(s): Router
  Type: Static
  Nexthop index: 0

T10, 00:19:e2:50:63:e0
  Interface(s): ge-0/0/46.0
  Type: Learn, Age: 0, Learned: 2:03:08
  Nexthop index: 0

T10, 00:19:e2:50:7d:e0
  Interface(s): Router
  Type: Static
  Nexthop index: 0

T111, *
  Interface(s): ge-0/0/15.0
  Type: Flood
  Nexthop index: 0
[output truncated]

show ethernet-switching table extensive
user@switch> show ethernet-switching table extensive
Ethernet-switching table: 57 entries, 17 learned
F2, *
  Interface(s): ge-0/0/44.0
  Type: Flood
  Nexthop index: 0

F2, 00:00:05:00:00:03

```

```

Interface(s): ge-0/0/44.0
Type: Learn, Age: 0, Learned: 2:03:09
Nexthop index: 0

F2, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Nexthop index: 0

Linux, *
Interface(s): ge-0/0/47.0
Type: Flood
Nexthop index: 0

Linux, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Nexthop index: 0

Linux, 00:30:48:90:54:89
Interface(s): ge-0/0/47.0
Type: Learn, Age: 0, Learned: 2:03:08
Nexthop index: 0

T1, *
Interface(s): ge-0/0/46.0
Type: Flood
Nexthop index: 0

T1, 00:00:05:00:00:01
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
Nexthop index: 0

T1, 00:00:5e:00:01:00
Interface(s): Router
Type: Static
Nexthop index: 0

T1, 00:19:e2:50:63:e0
Interface(s): ge-0/0/46.0
Type: Learn, Age: 0, Learned: 2:03:07
Nexthop index: 0

T1, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Nexthop index: 0

T10, *
Interface(s): ge-0/0/46.0
Type: Flood
Nexthop index: 0

T10, 00:00:5e:00:01:09
Interface(s): Router
Type: Static
Nexthop index: 0

T10, 00:19:e2:50:63:e0
Interface(s): ge-0/0/46.0

```

```
Type: Learn, Age: 0, Learned: 2:03:08
Nexthop index: 0

T10, 00:19:e2:50:7d:e0
Interface(s): Router
Type: Static
Nexthop index: 0

T111, *
Interface(s): ge-0/0/15.0
Type: Flood
Nexthop index: 0
[output truncated]
```

**show ethernet-switching
table interface ge-0/0/1**

```
user@switch> show ethernet-switching table interface ge-0/0/1
Ethernet-switching table: 1 unicast entries
VLAN          MAC address      Type      Age Interfaces
V1            *                Flood     - All-members
V1            00:00:05:00:00:05 Learn     0 ge-0/0/1.0
```