




Junos[®] OS for EX Series Ethernet Switches, Release 11.1: Device Security



Published: 2011-07-07
Revision 4

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 for EX Series Ethernet Switches, Release 11.1: Device Security

Copyright © 2011, Juniper Networks, Inc.

All rights reserved.

Writing:
Editing:
Illustration:
Cover Design:

Revision History
July 2011—Revision 4
May 2011—Revision 3
April 2011—Revision 2
March 2011—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 OS Release 11.1	ix
	Downloading Software	xi
	Documentation Symbols Key	xii
	Documentation Feedback	xiii
	Requesting Technical Support	xiv
	Self-Help Online Tools and Resources	xiv
	Opening a Case with JTAC	xiv
Part 1	Rate Limiting	
Chapter 1	Rate Limiting Overview	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	7
	Configuring Unknown Unicast Forwarding (CLI Procedure)	7
	Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)	8
Chapter 4	Verifying Rate Limiting Configuration	9
	Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface	9
	Verifying That the Port Error Disable Setting Is Working Correctly	10
Chapter 5	Configuration Statements for Rate Limiting	11
	[edit ethernet-switching-options] Configuration Statement Hierarchy	11
	action-shutdown	14
	bandwidth	15
	disable-timeout	16
	ethernet-switching-options	17
	interface	20
	interface	21
	no-broadcast	21
	no-multicast	22
	no-registered-multicast	22
	no-unknown-unicast	23
	no-unregistered-multicast	23

	port-error-disable	24
	storm-control	25
	unknown-unicast-forwarding	26
	vlan	27
Chapter 6	Operational Commands for Rate Limiting	29
	show ethernet-switching interfaces	30
	show ethernet-switching table	34

About This Topic Collection

- How to Use This Guide on page ix
- List of EX Series Guides for Junos OS Release 11.1 on page ix
- Downloading Software on page xi
- Documentation Symbols Key on page xii
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiv

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/junos11.1/information-products/topic-collections/release-notes/11.1/junos-release-notes-11.1.pdf.

List of EX Series Guides for Junos OS Release 11.1

Title	Description
<i>Complete Hardware Guide for EX2200 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX2200 Ethernet switches
<i>Complete Hardware Guide for EX3200 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX3200 Ethernet switches
<i>Complete Hardware Guide for EX4200 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX4200 Ethernet switches
<i>Complete Hardware Guide for EX4500 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX4500 Ethernet switches





Title	Description
<i>Complete Hardware Guide for EX8208 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8208 Ethernet switches
<i>Complete Hardware Guide for EX8216 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8216 Ethernet switches
<i>Complete Hardware Guide for the XRE200 External Routing Engine</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for the XRE200 External Routing Engine
<i>Complete Software Guide for Junos® OS for EX Series Ethernet Switches, Release 11.1</i>	Software feature descriptions, configuration examples, and tasks for Junos OS for EX Series switches
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 for Junos® OS for EX Series Ethernet Switches, Release 11.1</i> .)
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: Access Control</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: Configuration Management</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: Class of Service</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: Device Security</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: Ethernet Switching</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: EX4200 and EX4500 Virtual Chassis</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: EX8200 Virtual Chassis</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: Fibre Channel over Ethernet</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: High Availability</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: Interfaces</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: Layer 3 Protocols</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: MPLS</i>	

Title	Description
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: Multicast</i>	
<i>Junos® OS for EX Series Switches, Release 11.1: Network Management and Monitoring</i>	
<i>Junos® OS for EX Series Switches, Release 11.1: Port Security</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: Routing Policy and Packet Filtering</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: Software Installation</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: Spanning-Tree Protocols</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: System Monitoring</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: System Services</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: System Setup</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: User and Access Management</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.1: User Interfaces</i>	

Downloading Software

You can download Junos OS 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 configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<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 OS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
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 stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;

Text and Syntax Conventions		
Convention	Description	Examples
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast <i>(string1 string2 string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
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/us/en/local/pdf/resource-guides/7100059-en.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Rate Limiting

- Rate Limiting Overview on page 3
- Example: Rate Limiting Configuration on page 5
- Configuring Rate Limiting on page 7
- Verifying Rate Limiting Configuration on page 9
- Configuration Statements for Rate Limiting on page 11
- Operational Commands for Rate Limiting on page 29

CHAPTER 1

Rate Limiting Overview

- 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 to drop broadcast, multicast, 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. As an alternative to having the switch drop packets, you can configure it to shut down interfaces or temporarily disable interfaces (see the **action-shutdown** statement or the **port-error-disable** statement) when the storm control level is exceeded.

The factory default configuration enables storm control on all switch interfaces, with the storm control level set to 80 percent of the combined broadcast, multicast, and unknown unicast streams. You can change the storm control level for an interface by specifying a bandwidth value for the combined broadcast, multicast, and unknown unicast traffic streams. You can also selectively disable storm control on the broadcast stream, on the multicast stream, or on the unknown unicast stream.



NOTE: On EX8200 switches, you can also selectively disable storm control on registered multicast traffic, on unregistered multicast traffic, or on both types of multicast traffic.

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 level of broadcast, multicast, and unknown unicast traffic in the LAN when it is operating normally. Use this data as a benchmark to determine when traffic levels

are too high. Then configure storm control to set the level at which you want to drop broadcast traffic, multicast traffic, unknown unicast traffic, or two or all three of those traffic types.



NOTE: When you configure storm control bandwidth on an aggregated Ethernet interface, the storm control level for each member of the aggregated Ethernet interface is set to that bandwidth. For example, if you configure a storm control bandwidth of 15,000 Kbps on ae1, and ae1 has two members, ge-0/0/0 and ge-0/0/1, each member has a storm control level of 15,000 Kbps. Thus, the storm control level on ae1 allows a traffic rate of up to 30,000 Kbps of combined broadcast, multicast, and unknown unicast traffic.

**Related
Documentation**

- 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 8
- Disabling or Enabling Storm Control (CLI Procedure)

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 all unknown unicast traffic to a specific trunk interface. This channels the unknown unicast traffic to a single interface.

**Related
Documentation**

- 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 7

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, multicast 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 on page 6

Requirements

This example uses the following hardware and software components:

- One EX Series switch
- Junos OS Release 9.5 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, multicast traffic, and unknown unicast traffic to be allowed on an interface. You specify the storm control level as the traffic rate in kilobits per second of the combined broadcast, multicast, and unknown unicast streams.



NOTE: The factory default configuration enables storm control on all interfaces at 80 percent of the combined broadcast, multicast, and unknown unicast streams.

Storm control monitors the incoming broadcast traffic, multicast traffic, and unknown unicast traffic and compares it with the level that you specify. If broadcast traffic, multicast traffic, and unknown unicast traffic exceed the specified level, the switch drops packets for the controlled traffic types. As an alternative to having the switch drop packets, you can configure it to shut down interfaces or temporarily disable interfaces (see the **action-shutdown** statement or the **port-error-disable** statement) when the storm control level is exceeded.

The topology used in this example consists of one EX Series 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 setting the level to a traffic rate of 15,000 Kbps, based on the traffic rate of the combined broadcast, multicast, and unknown unicast streams. If broadcast traffic, multicast traffic, and unknown unicast traffic exceeds this level, the switch drops packets for the controlled traffic types to prevent a network outage.

Configuration

CLI Quick Configuration

To quickly configure storm control based on the traffic rate in kilobits per second of the combined broadcast, multicast, 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:

1. Specify the traffic rate in kilobits per second of the combined broadcast, multicast, and unknown unicast streams 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;
}
```

Related Documentation

- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 8
- Understanding Storm Control on EX Series Switches on page 3

CHAPTER 3

Configuring Rate Limiting

- Configuring Unknown Unicast Forwarding (CLI Procedure) on page 7
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 8

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:



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 Documentation

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5
- Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface on page 9
- 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 Documentation

- 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 9
- Verifying That the Port Error Disable Setting Is Working Correctly on page 10

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 Documentation**
- Configuring Unknown Unicast Forwarding (CLI Procedure) on page 7

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 Documentation**
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 8

CHAPTER 5

Configuration Statements for Rate Limiting

- [edit ethernet-switching-options] Configuration Statement Hierarchy on page 11

[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-notification {
  notification-interval seconds;
}
mac-table-aging-time seconds;
port-error-disable {
```

```
    disable-timeout timeout;
  }
  redundant-trunk-group {
    group name {
      preempt-cutover-timer seconds;
      interface
        primary;
      }
    interface
    }
  }
  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 );
      fcoe-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 );
    examine-fip {
      fc-map fc-map-value;
    }
    (ip-source-guard | no-ip-source-guard);
    mac-move-limit limit action action;
  }
}
static {
  vlan name {
    mac mac-address {
```

```

        next-hop interface-name;
    }
}
storm-control {
    action-shutdown;
    interface (all | interface-name) {
        bandwidth bandwidth;
        no-broadcast;
        no-multicast;
        no-registered-multicast;
        no-unknown-unicast;
        no-unregistered-multicast;
    }
}
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 Documentation

- [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](#)
- [Understanding MAC Notification on EX Series Switches](#)
- [Understanding FIP Snooping](#)

action-shutdown

Syntax	action-shutdown;
Hierarchy Level	[edit ethernet-switching-options storm-control]
Release Information	Statement introduced in Junos OS 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, multicast, and broadcast messages on the specified interfaces.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• port-error-disable on page 24• disable-timeout on page 16• 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 8• Understanding Storm Control on EX Series Switches on page 3

bandwidth

Syntax	<code>bandwidth <i>bandwidth</i>;</code>
Hierarchy Level	<code>[edit ethernet-switching-options storm-control interface (all <i>interface-name</i>)]</code>
Release Information	Statement introduced in Junos OS Release 9.5 for EX Series switches.
Description	Configure the storm control level as the bandwidth in kilobits per second of the combined broadcast, multicast, and unknown unicast streams.
	<div>  <p>NOTE: When you configure storm control bandwidth on an aggregated Ethernet interface, the storm control level for each member of the aggregated Ethernet interface is set to that bandwidth. For example, if you configure a storm control bandwidth of 15,000 Kbps on ae1, and ae1 has two members, ge-0/0/0 and ge-0/0/1, each member has a storm control level of 15,000 Kbps. Thus, the storm control level on ae1 allows a traffic rate of up to 30,000 Kbps of combined broadcast, multicast, and unknown unicast traffic.</p> </div>
Default	If you omit the bandwidth statement when you configure storm control on an interface, the storm control level defaults to 80 percent of the combined broadcast, multicast, and unknown unicast streams.
Options	<p>bandwidth—Traffic rate in kilobits per second of the combined broadcast, multicast, and unknown unicast streams.</p> <p>Range: 100 through 100000000</p> <p>Default: None</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<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	<code>disable-timeout <i>timeout</i>;</code>
Hierarchy Level	<code>[edit ethernet-switching-options port-error-disable]</code>
Release Information	Statement introduced in Junos OS 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 Documentation	<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 8• 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-notification {
            notification-interval seconds;
        }
        mac-table-aging-time seconds;
        port-error-disable {
            disable-timeout timeout;
        }
        redundant-trunk-group {
            group 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);
    fcoe-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);
    examine-fip {
        fc-map fc-map-value;
    }
    (ip-source-guard | no-ip-source-guard);
    mac-move-limit limit action action;
}
static {
    vlan name {
        mac mac-address {
            next-hop interface-name;
        }
    }
}
storm-control {
    action-shutdown;
    interface (all | interface-name) {
        bandwidth bandwidth;
        no-broadcast;
        no-multicast;
        no-registered-multicast;
        no-unknown-unicast;
        no-unregistered-multicast;
    }
}
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 OS Release 9.0 for EX Series switches.

Description Configure Ethernet switching options.

The remaining statements are explained separately.

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

Related Documentation

- [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](#)
- [Understanding MAC Notification on EX Series Switches](#)
- [Understanding FIP Snooping](#)

interface

Syntax	<pre>interface (all <i>interface-name</i>) { bandwidth <i>bandwidth</i>; no-broadcast; no-multicast; no-registered-multicast; no-unknown-unicast; no-unregistered-multicast; }</pre>
Hierarchy Level	[edit ethernet-switching-options storm-control]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	<p>Enable and configure storm control on all interfaces or on the specified interface.</p> <p>If you do not include the bandwidth statement, the storm control level defaults to 80 percent of the combined broadcast, multicast, and unknown unicast streams.</p>
Default	The factory default configuration enables storm control on all switch interfaces at the default level of 80 percent of the combined broadcast, multicast, and unknown unicast streams.
Options	<p>all—All interfaces. The storm control settings configured with the all option affect only those interfaces that have not been individually configured for storm control.</p> <p><i>interface-name</i>—Name of an interface. The storm control settings configured with the <i>interface-name</i> option override any settings configured with the all option.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<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

interface

Syntax	<code>interface <i>interface-name</i>;</code>
Hierarchy Level	<code>[edit ethernet-switching-options unknown-unicast-forwarding vlan(all <i>vlan-name</i>)]</code>
Release Information	Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	Specify the interface to which unknown unicast packets will be forwarded.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <code>show vlans</code> • show ethernet-switching table on page 34 • Configuring Unknown Unicast Forwarding (CLI Procedure) on page 7 • Understanding Unknown Unicast Forwarding on EX Series Switches on page 4

no-broadcast

Syntax	<code>no-broadcast;</code>
Hierarchy Level	<code>[edit ethernet-switching-options storm-control interface (all <i>interface-name</i>)]</code>
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Disable storm control for broadcast traffic for the specified interface or for all interfaces.
Default	Storm control is enabled for broadcast traffic.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<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-multicast

Syntax	no-multicast;
Hierarchy Level	[edit ethernet-switching-options storm-control interface (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 10.3 for EX Series switches.
Description	Disable storm control for all multicast traffic (both registered multicast and unregistered multicast) for the specified interface or for all interfaces.
Default	Storm control is enabled for unknown unicast traffic, multicast traffic, and broadcast traffic.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• no-registered-multicast on page 22• no-unregistered-multicast on page 23• Understanding Storm Control on EX Series Switches on page 3

no-registered-multicast

Syntax	no-registered-multicast;
Hierarchy Level	[edit ethernet-switching-options storm-control interface (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 10.3 for EX Series switches.
Description	(EX8200 switches only) Disable storm control for registered multicast traffic for the specified interface or for all interfaces.
Default	Storm control is enabled for unknown unicast traffic, multicast traffic, and broadcast traffic.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• no-multicast on page 22• no-unregistered-multicast on page 23• 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 <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Disable storm control for unknown unicast traffic for the specified interface or for all interfaces.
Default	Storm control is enabled for unknown unicast traffic.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • no-unregistered-multicast on page 23 • 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-unregistered-multicast

Syntax	no-unregistered-multicast;
Hierarchy Level	[edit ethernet-switching-options storm-control interface (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 10.3 for EX Series switches.
Description	(EX8200 switches only) Disable storm control for unregistered multicast traffic for the specified interface or for all interfaces.
Default	Storm control is enabled for unknown unicast traffic, multicast traffic, and broadcast traffic.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • no-multicast on page 22 • no-registered-multicast on page 22 • Understanding Storm Control on EX Series Switches on page 3

port-error-disable

Syntax	<pre>port-error-disable { disable-timeout <i>timeout</i> ; }</pre>
Hierarchy Level	[edit ethernet-switching-options]
Release Information	Statement introduced in Junos OS Release 9.6 for EX Series switches.
Description	<p>Disable rather than block an interface when enforcing MAC limiting, MAC move limiting, and rate-limiting configuration options for shutting down the interface, and allow the interface to recover automatically from the error condition after a specified period of time:</p> <ul style="list-style-type: none">• If you have enabled mac-limit with the shutdown option and enable port-error-disable, the switch disables (rather than shuts down) the interface when the MAC address limit is reached.• If you have enabled mac-move-limit with the shutdown option and you enable port-error-disable, the switch disables (rather than shuts down) the interface when the maximum number of moves to a new interface is reached.• If you have enabled storm-control with the action-shutdown option and you enable port-error-disable, the switch disables (rather than shuts down) the interface when broadcast traffic, multicast traffic, and unknown unicast traffic exceeds the specified levels.
	<div><p>NOTE: The port-error-disable configuration does not apply to pre-existing error conditions. It impacts only error conditions that are detected after port-error-disable has been enabled and committed. To clear a pre-existing error condition and restore the interface to service, use the clear ethernet-switching port-error command.</p></div>
Default	Not enabled.
Required Privilege Level	system—To view this statement in the configuration. system—control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 8• Configuring Port Security (CLI Procedure)• Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 5

storm-control

Syntax	<pre>storm-control { action-shutdown; interface (all <i>interface-name</i>) { bandwidth <i>bandwidth</i>; no-broadcast; no-multicast; no-registered-multicast; no-unknown-unicast; no-unregistered-multicast; } }</pre>
Hierarchy Level	[edit ethernet-switching-options]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	<p>Configure storm control on the switch.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<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

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 OS 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 system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Documentation

- show vlans
- **show ethernet-switching table on page 34**
- Configuring Unknown Unicast Forwarding (CLI Procedure) on page 7
- 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 OS Release 9.3 for EX Series switches.
Statement updated with enhanced ? (CLI completion feature) functionality in Junos OS 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 `vlands` 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 `system`—To view this statement in the configuration.
`system-control`—To add this statement to the configuration.

Related Documentation

- `show vlans`
- **show ethernet-switching table on page 34**
- Configuring Unknown Unicast Forwarding (CLI Procedure) on page 7
- Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface on page 9
- Understanding Unknown Unicast Forwarding on EX Series Switches on page 4

CHAPTER 6

Operational Commands for Rate Limiting

show ethernet-switching interfaces

Syntax	<code>show ethernet-switching interfaces</code> <code><brief detail summary></code> <code><interface <i>interface-name</i>></code>
Release Information	<p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>In Junos OS Release 9.6 for EX Series switches, the following updates were made:</p> <ul style="list-style-type: none">• Blocking field output was updated.• The default view was updated to include information about 802.1Q tags.• The detail view was updated to include information on VLAN mapping. <p>In Junos OS Release 11.1 for EX Series switches, the detail view was updated to include reflective relay information.</p>
Description	Display information about Ethernet switching interfaces.
Options	<p><code>none</code>—Display brief information for Ethernet switching interfaces.</p> <p><code>brief detail summary</code>—(Optional) Display the specified level of output.</p> <p><code>interface <i>interface-name</i></code>—(Optional) Display Ethernet switching information for a specific interface.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <code>show ethernet-switching mac-learning-log</code>• show ethernet-switching table on page 34• Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 8
List of Sample Output	<p><code>show ethernet-switching interfaces</code> on page 32</p> <p><code>show ethernet-switching interfaces ge-0/0/15 brief</code> on page 32</p> <p><code>show ethernet-switching interfaces ge-0/0/2 detail</code> (Blocked by RTG rtggroup) on page 32</p> <p><code>show ethernet-switching interfaces ge-0/0/15 detail</code> (Blocked by STP) on page 33</p> <p><code>show ethernet-switching interfaces ge-0/0/17 detail</code> (Disabled by bpdu-control) on page 33</p> <p><code>show ethernet-switching interfaces detail</code> (C-VLAN to S-VLAN Mapping) on page 33</p> <p><code>show ethernet-switching interfaces detail</code> (reflective relay is configured) on page 33</p>
Output Fields	Table 1 on page 31 lists the output fields for the <code>show ethernet-switching interfaces</code> 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.	none, brief , detail , summary
Index	VLAN index internal to Junos OS.	detail
State	Interface state. Values are up and down .	none, brief , detail
Port mode	Access mode is the port mode default and works with a single VLAN. Port mode can also be trunk , which accepts tagged packets from multiple VLANs on other switches. The third port mode value is tagged-access which accepts tagged packets from access devices.	detail
Reflective Relay Status	Reflective relay allows packets to use the same interface for both upstream and downstream traffic. When reflective relay has been configured, the status displayed is always enabled . When reflective relay is not configured, this entry does not appear in the command output.	detail
Ethertype for the interface	EtherType is a two-octet field in an Ethernet frame used to indicate which protocol is encapsulated in the payload of an incoming Ethernet packet. Both 802.1Q packets and Q in Q packets use this field. The output displayed for this particular field indicates the interface's ethertype which is used to match the ethertype of incoming 802.1Q packets and Q in Q packets. The indicated ethertype field is also added to the interface's outgoing 802.1Q and Q in Q packets.	detail
VLAN membership	Names of VLANs that belong to this interface.	none, brief , detail ,
Tag	Number of the 802.1Q-tag.	none, brief , detail ,
Tagging	Specifies whether the interface forwards 802.1Q tagged or untagged traffic.	none, brief , detail ,
Blocking	<p>The forwarding state of the interface:</p> <ul style="list-style-type: none"> • unblocked—Traffic is forwarded on the interface. • blocked—Traffic is not being forwarded on the interface. • Disabled by bpdud control—The interface is disabled due to receiving BPDUs on a protected interface. If the disable-timeout statement has been included in the BPDUD 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 ,

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

Field Name	Field Description	Level of Output
Number of MACs learned on IFL	Number of MAC addresses learned by this interface.	detail
mapping	<p>When mapping is configured, the status is one of the following C-VLAN to S-VLAN mapping types:</p> <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. <p>When mapping is not configured, this entry does not appear in the command output.</p>	detail

Sample Output

```

show user@switch> show ethernet-switching interfaces
ethernet-switching
interfaces
Interface      State  VLAN members      Tag  Tagging  Blocking
-----
ae0.0          up     default
ge-0/0/2.0     up     vlan300           300  untagged unblocked
ge-0/0/3.0     up     default           300  untagged blocked by RTG (rtggroup)
ge-0/0/4.0     down   default           300  untagged blocked by STP
ge-0/0/5.0     down   default           300  untagged MAC limit exceeded
ge-0/0/6.0     down   default           300  untagged MAC move limit exceeded
ge-0/0/7.0     down   default           300  untagged Storm control in effect
ge-0/0/13.0    up     default           300  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           100  untagged unblocked
ge-0/0/17.0    down   vlan100           100  tagged  Disabled by bpdu-control
               vlan200           200  tagged  Disabled by bpdu-control

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

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

```

Number of MACs learned on IFL: 0

```

show user@switch> show ethernet-switching interfaces ge-0/0/15 detail
ethernet-switching
interfaces ge-0/0/15
detail (Blocked by
      STP)
      Interface: ge-0/0/15.0, Index: 70, State: up, Port mode: Trunk
      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 user@switch> show ethernet-switching interfaces ge-0/0/17 detail
ethernet-switching
interfaces ge-0/0/17
detail (Disabled by
      bpdu-control)
      Interface: ge-0/0/17.0, Index: 71, State: down, Port mode: Trunk
      VLAN membership:
        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 user@switch> show ethernet-switching interfaces ge-0/0/6.0 detail
ethernet-switching
interfaces detail
(C-VLAN to S-VLAN
      Mapping)
      Interface: ge-0/0/6.0, Index: 73, State: up, Port mode: Access
      VLAN membership:
        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 user@switch1> show ethernet-switching interfaces ge-7/0/2 detail
ethernet-switching
interfaces detail
(reflective relay is
      configured)
      Interface: ge-7/0/2, Index: 66, State: down, Port mode: Tagged-access
      Reflective Relay Status: Enabled
      Ether type for the interface: 0x8100
      VLAN membership:
        VLAN_Purple VLAN_Orange VLAN_Blue, 802.1Q Tag: 450, tagged, unblocked
      Number of MACs learned on IFL: 0

```

show ethernet-switching table

Syntax	<code>show ethernet-switching table</code> <code><brief detail extensive summary></code> <code><interface <i>interface-name</i>></code> <code><management-vlan></code> <code><sort-by (<i>name</i> <i>tag</i>)></code> <code><vlan <i>vlan-name</i>></code>
Release Information	Command introduced in Junos OS Release 9.0 for EX Series switches. Options summary , management-vlan , and vlan <i>vlan-name</i> introduced in Junos OS Release 9.6 for EX Series switches. Option sort-by and field name tag introduced in Junos OS Release 10.1 for EX Series switches.
Description	Display the Ethernet switching table.
Options	<code>none</code> —(Optional) Display brief information about the Ethernet switching table. <code>brief detail extensive summary</code> —(Optional) Display the specified level of output. <code>interface <i>interface-name</i></code> —(Optional) Display the Ethernet switching table for a specific interface. <code>management-vlan</code> —(Optional) Display the Ethernet switching table for a management VLAN. <code>sort-by (<i>name</i> <i>tag</i>)</code> —(Optional) Display VLANs in ascending order of VLAN IDs or VLAN names. <code>vlan <i>vlan-name</i></code> —(Optional) Display the Ethernet switching table for a specific VLAN.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• clear ethernet-switching table• 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	<code>show ethernet-switching table</code> on page 35 <code>show ethernet-switching table brief</code> on page 36 <code>show ethernet-switching table detail</code> on page 36 <code>show ethernet-switching table extensive</code> on page 37 <code>show ethernet-switching table interface ge-0/0/1</code> on page 37
Output Fields	Table 2 on page 35 lists the output fields for the show ethernet-switching table 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
Tag	The VLAN ID tag name or number.	extensive
MAC or MAC address	The MAC address associated with the VLAN.	All levels
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
Nexthop index	The next-hop index number.	detail, extensive

Sample Output

```

show user@switch> show ethernet-switching table
ethernet-switching Ethernet-switching table: 57 entries, 17 learned
table
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 user@switch> show ethernet-switching table brief
ethernet-switching Ethernet-switching table: 57 entries, 17 learned
table brief
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 user@switch> show ethernet-switching table detail
ethernet-switching Ethernet-switching table: 5 entries, 2 learned
table detail
VLAN: default, Tag: 0, MAC: *, Interface: All-members
Interfaces:
  ge-0/0/11.0, ge-0/0/20.0, ge-0/0/30.0, ge-0/0/36.0, ge-0/0/3.0
Type: Flood
Nextthop index: 1307

VLAN: default, Tag: 0, MAC: 00:1f:12:30:b8:83, Interface: ge-0/0/3.0
Type: Learn, Age: 0, Learned: 20:09:26
Nextthop index: 1315

VLAN: v1, Tag: 101, MAC: *, Interface: All-members
Interfaces:
  ge-0/0/31.0
Type: Flood
Nextthop index: 1313

```

```
VLAN: v1, Tag: 101, MAC: 00:1f:12:30:b8:89, Interface: ge-0/0/31.0
Type: Learn, Age: 0, Learned: 20:09:25
Nexthop index: 1312
```

```
VLAN: v2, Tag: 102, MAC: *, Interface: All-members
Interfaces:
  ae0.0
Type: Flood
Nexthop index: 1317
```

**show
ethernet-switching
table extensive**

```
user@switch> show ethernet-switching table extensive
Ethernet-switching table: 3 entries, 1 learned
```

```
VLAN: v1, Tag: 10, MAC: *, Interface: All-members
Interfaces:
  ge-0/0/14.0, ge-0/0/1.0, ge-0/0/2.0, ge-0/0/3.0, ge-0/0/4.0,
  ge-0/0/5.0, ge-0/0/6.0, ge-0/0/7.0, ge-0/0/8.0, ge-0/0/10.0,
  ge-0/0/0.0
Type: Flood
Nexthop index: 567

VLAN: v1, Tag: 10, MAC: 00:21:59:c6:93:22, Interface: Router
Type: Static
Nexthop index: 0

VLAN: v1, Tag: 10, MAC: 00:21:59:c9:9a:4e, Interface: ge-0/0/14.0
Type: Learn, Age: 0, Learned: 18:40:50
Nexthop index: 564
```

**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

