



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

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: Multicast

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 NON-INFRINGEMENT. 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	IGMP Snooping and Multicast	
Chapter 1	Understanding IGMP Snooping and Multicast	3
	IGMP Snooping on EX Series Switches Overview	3
	How IGMP Snooping Works	3
	How IGMP Snooping Works with Routed VLAN Interfaces	4
	How Hosts Join and Leave Multicast Groups	7
	IGMP Snooping Support for IGMPv3	7
	Understanding Multicast VLAN Registration on EX Series Switches	8
	How MVR Works	8
	MVR Modes	9
Chapter 2	Examples: GMP Snooping and Multicast Configuration	11
	Example: Configuring IGMP Snooping on EX Series Switches	11
	Example: Configuring Multicast VLAN Registration on EX Series Switches	14
Chapter 3	Configuring IGMP Snooping and Multicast	19
	Configuring IGMP Snooping (CLI Procedure)	19
	Configuring IGMP Snooping (J-Web Procedure)	20
	Changing the IGMP Snooping Group Query Membership Timeout Value (CLI Procedure)	23
	Configuring Multicast VLAN Registration (CLI Procedure)	24

Chapter 4	Verifying IGMP Snooping and Multicast	27
	Monitoring IGMP Snooping	27
	Verifying That the IGMP Snooping Group Query Timeout Value Has Been Changed Correctly	28
Chapter 5	Configuration Statements for IGMP Snooping and Multicast	31
	[edit protocols] Configuration Statement Hierarchy	31
	data-forwarding	37
	disable	38
	group	38
	groups	39
	group-limit	40
	igmp-snooping	41
	immediate-leave	42
	install	43
	interface	44
	multicast-router-interface	44
	proxy	45
	query-interval	46
	query-last-member-interval	47
	query-response-interval	48
	receiver	49
	robust-count	49
	source	50
	source-vlans	50
	traceoptions	51
	vlan	53
Chapter 6	Operational Mode Commands for IGMP Snooping and Multicast	55
	clear igmp-snooping membership	56
	clear igmp-snooping statistics	57
	show igmp-snooping membership	58
	show igmp-snooping route	61
	show igmp-snooping statistics	63
	show igmp-snooping vlans	64

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](http://www.juniper.net/support/requesting%20support.html) .

Part 1

IGMP Snooping and Multicast

- Understanding IGMP Snooping and Multicast on page 3
- Examples: IGMP Snooping and Multicast Configuration on page 11
- Configuring IGMP Snooping and Multicast on page 19
- Verifying IGMP Snooping and Multicast on page 27
- Configuration Statements for IGMP Snooping and Multicast on page 31
- Operational Mode Commands for IGMP Snooping and Multicast on page 55

Chapter 1

Understanding IGMP Snooping and Multicast

- IGMP Snooping on EX Series Switches Overview on page 3
- Understanding Multicast VLAN Registration on EX Series Switches on page 8

IGMP Snooping on EX Series Switches Overview

Internet Group Management Protocol (IGMP) snooping regulates multicast traffic in a switched network. With IGMP snooping enabled, a LAN switch monitors the IGMP transmissions between a host (a network device) and a multicast router, keeping track of the multicast groups and associated member interfaces. The switch uses that information to make intelligent multicast-forwarding decisions and forward traffic to the intended destination interfaces. Juniper Networks EX Series Ethernet Switches support IGMPv1, IGMPv2, and IGMPv3 (INCLUDE mode only).

For details on IGMPv1, IGMPv2, and IGMPv3, see the following standards:

- For IGMPv1, see RFC 1112, *Host extensions for IP multicasting* at <http://www.faqs.org/rfcs/rfc1112.html>.
- For IGMPv2, see RFC 2236, *Internet Group Management Protocol, Version 2* at <http://www.faqs.org/rfcs/rfc2236.html>.
- For IGMPv3, see RFC 3376, *Internet Group Management Protocol, Version 3* at <http://www.faqs.org/rfcs/rfc3376.html>.

This IGMP snooping topic covers:

- How IGMP Snooping Works on page 3
- How IGMP Snooping Works with Routed VLAN Interfaces on page 4
- How Hosts Join and Leave Multicast Groups on page 7
- IGMP Snooping Support for IGMPv3 on page 7

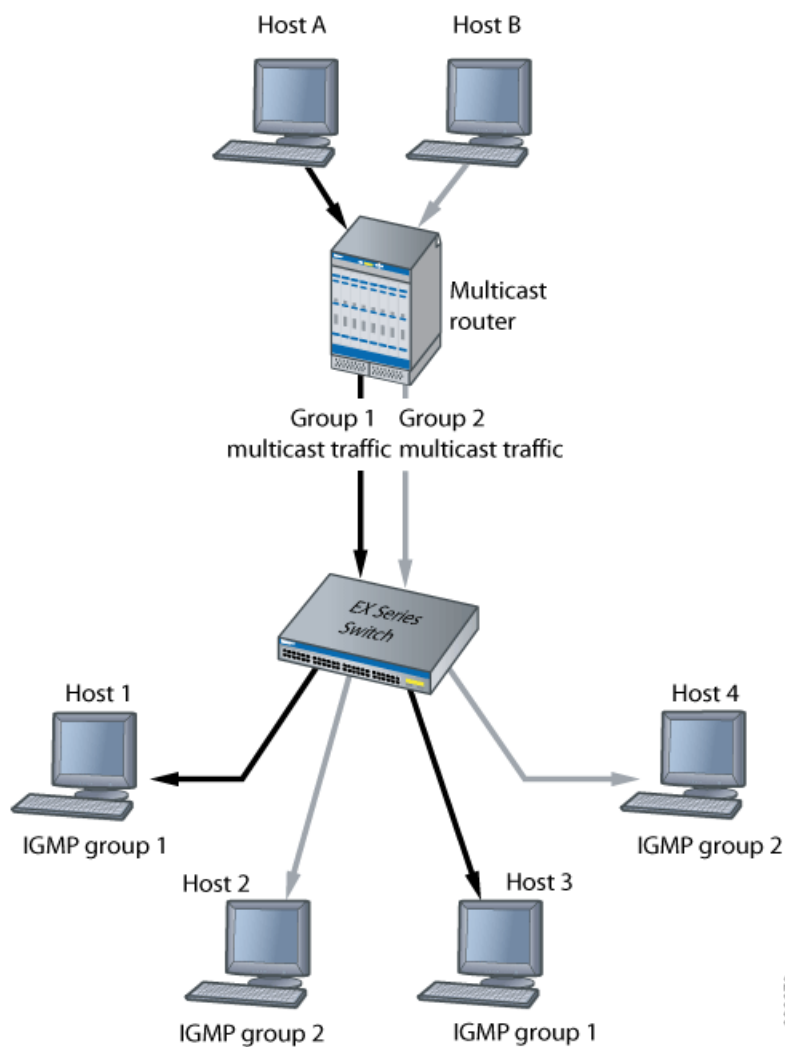
How IGMP Snooping Works

An EX Series switch usually learns *unicast* MAC addresses by checking the source address field of the frames it receives. However, a *multicast* MAC address can never be the source address for a packet. As a result, the switch floods multicast traffic on the VLAN, consuming significant amounts of bandwidth.

IGMP snooping regulates multicast traffic on a VLAN to avoid flooding. When IGMP snooping is enabled, the switch intercepts IGMP packets and uses the content of the packets to build a multicast cache table. The cache table is a database of multicast groups and their corresponding member ports. The cache table is then used to regulate multicast traffic on the VLAN.

When the switch receives multicast packets, it uses the cache table to selectively forward the packets only to the ports that are members of the destination multicast group. Figure 1 on page 4 shows an example of IGMP traffic flow with IGMP snooping enabled.

Figure 1: IGMP Traffic Flow with IGMP Snooping Enabled



How IGMP Snooping Works with Routed VLAN Interfaces

Switches send traffic to hosts that are part of the same broadcast domain, but routers are needed to route traffic from one broadcast domain to another. EX Series switches

use a routed VLAN interface (RVI) to perform these routing functions. IGMP snooping works with Layer 2 interfaces and RVIs to regulate multicast traffic in a switched network.

When an EX Series switch receives a multicast packet, the Packet Forwarding Engines in the switch perform an IP multicast lookup on the multicast packet to determine how to forward the packet to its local ports. From the results of the IP multicast lookup, each Packet Forwarding Engine extracts a list of Layer 3 interfaces (which can include VLAN interfaces) that have ports local to the Packet Forwarding Engine. If an RVI is part of this list, the switch provides a bridge multicast group ID for each RVI to the Packet Forwarding Engine.

A bridge multicast ID is assigned to direct Layer 3 interfaces and to RVIs. For VLANs that include multicast receivers, the bridge multicast ID includes a sub-next-hop ID. The sub-next-hop ID identifies the multicast Layer 2 interfaces in that VLAN that are interested in receiving the multicast stream. The switch ultimately assigns a next hop after it does a route lookup. The next hop includes all direct Layer 3 interfaces and RVIs. The Packet Forwarding Engine then forwards multicast traffic to the bridge multicast ID that includes all Layer 3 interfaces and RVIs that are multicast receivers for a given multicast group.

Figure 2 on page 6 shows how multicast traffic is forwarded on a multilayer switch. In this illustration, multicast traffic is coming in through the `xe-0/1/0.0` interface. A multicast group has been formed by the Layer 3 interface `ge-0/0/2.0`, `vlan.0`, and `vlan.1`. The `ge-2/0/0.0` interface is a common trunk interface that belongs to both `vlan.0` and `vlan.1`. The letter “R” next to an interface name in the illustration indicates that a multicast receiver host is associated with that interface.



NOTE: Traffic sent to an access interface is untagged; traffic sent to a trunk interface is tagged. For more information on VLAN tagging, see Understanding Bridging and VLANs on EX Series Switches.

Figure 2: IGMP Traffic Flow with Routed VLAN Interfaces

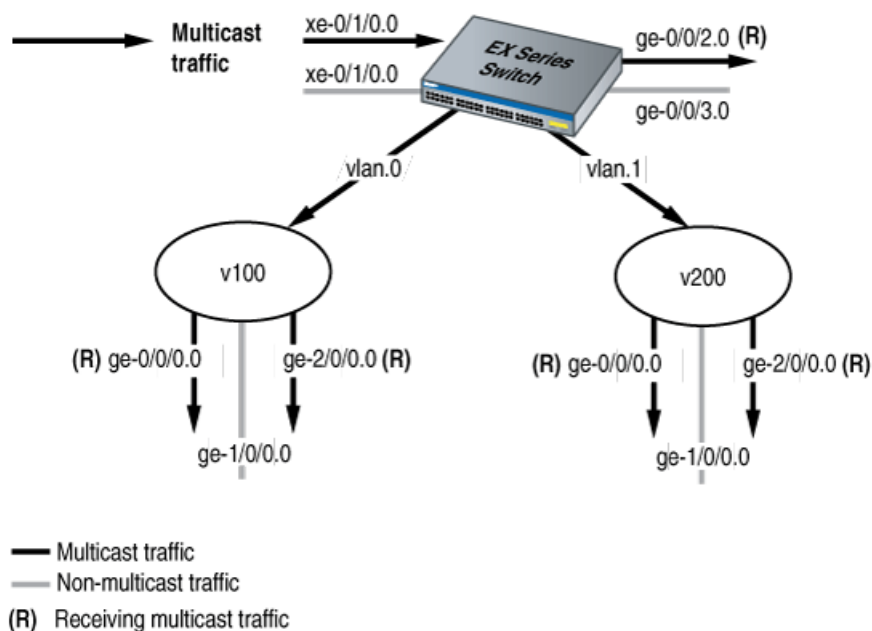


Table 1 on page 6 shows the bridge multicast IDs and next hops that are created. The term *subnh* refers to a sub-next hop. The Packet Forwarding Engine will forward multicast traffic to bridge multicast ID9.

Table 1: Bridge Multicast IDs and Next Hops

ID Number	Type of Next Hop	Next Hop	Tag Information
ID1	RHN_UNICAST	ge-0/0/0.0	tag = off
ID2	RHN_UNICAST	ge-2/0/0.0	tag = on
ID3	RHN_FLOOD	[ID1, ID2]	
ID4	RHN_UNICAST	ge-0/0/1.0	tag = off
ID5	RHN_FLOOD	[ID4, ID2]	
ID6	RHN_UNICAST	vlan.0	subnh = ID3
ID7	RHN_UNICAST	VLAN.1	subnh = ID5
ID8	RHN_UNICAST	ge-0/0/2.0	
ID9	RHN_FLOOD	[ID6, ID7, ID8]	

How Hosts Join and Leave Multicast Groups

Hosts can join multicast groups in either of two ways:

- By sending an unsolicited IGMP join message to a multicast router that specifies the IP multicast group that the host is attempting to join.
- By sending an IGMP join message in response to a general query from a multicast router.

A multicast router continues to forward multicast traffic to a VLAN provided that at least one host on that VLAN responds to the periodic general IGMP queries. For a host to remain a member of a multicast group, therefore, it must continue to respond to the periodic general IGMP queries.

To leave a multicast group, a host can either not respond to the periodic general IGMP queries, which results in a “silent leave” (the only leave option for hosts connected to switches running IGMPv1), or send a group-specific IGMPv2 leave message.

IGMP Snooping Support for IGMPv3

IGMPv3 allows IGMP snooping to filter multicast streams based on the source address of the multicast stream. JUNOS Software for EX Series switches supports IGMPv3 packets that are in INCLUDE mode only. IGMPv3 packets in any other mode are dropped.

When a host sends an IGMPv3 INCLUDE report through a switch interface to indicate that it wants to receive a multicast stream from a source address, the switch adds the source address to the source list. In INCLUDE mode, the switch requests that packets be sent to the specified multicast address only from those IP source addresses listed in the source-list parameter. However, because EX Series switches do not support forwarding on a per-source basis, the switch merges all IGMPv3 reports for a VLAN to create a (*,G,V) route with the appropriate next hop. This next hop contains all the interfaces on the VLAN that are interested in group G.

When IGMP snooping for IGMPv3 is used with an RVI, the same (*,G,V) route is added to the snooping information in the RVI's output interface list (olist).

- Related Topics**
- Understanding Multicast VLAN Registration on EX Series Switches on page 8
 - Example: Configuring IGMP Snooping on EX Series Switches on page 11
 - Configuring IGMP Snooping (CLI Procedure) on page 19
 - RFC 3171, *IANA Guidelines for IPv4 Multicast Address Assignments* at <http://tools.ietf.org/html/rfc3171>

Understanding Multicast VLAN Registration on EX Series Switches

Multicast VLAN registration (MVR) allows you to efficiently distribute IPTV multicast streams across an Ethernet ring-based Layer 2 network and reduce the amount of bandwidth consumed by this multicast traffic.

In a standard Layer 2 network, a multicast stream received on one VLAN is never distributed to interfaces outside that VLAN. If hosts in multiple VLANs request the same multicast stream, a separate copy of that multicast stream is distributed to the requesting VLANs.

MVR introduces the concept of a *multicast source VLAN* (MVLAN), which is created by MVR and becomes the only VLAN over which IPTV multicast traffic flows throughout the Layer 2 network. The Juniper Networks EX Series Ethernet Switch that is enabled for MVR selectively forward IPTV multicast traffic from interfaces on the MVLAN (source interfaces) to hosts that are connected to interfaces that are not part of the MVLAN. These interfaces are known as *MVR receiver ports*. The MVR receiver ports can receive traffic from a port on the MVLAN but cannot send traffic onto the MVLAN, and they remain in their own VLANs for bandwidth and security reasons.

This topic includes:

- How MVR Works on page 8

How MVR Works

In many ways, MVR is similar to IGMP snooping. Both monitor IGMP join and leave messages and build forwarding tables based on the media access control (MAC) addresses of the hosts sending those IGMP messages. Whereas IGMP snooping operates within a given VLAN to regulate multicast traffic, MVR can operate with hosts on different VLANs in a Layer 2 network to selectively deliver IPTV multicast traffic to requesting hosts, thereby reducing the amount of bandwidth needed to forward multicast traffic.

When you configure an MVLAN, you assign a range of multicast group addresses to it. You then configure other VLANs to be MVR receiver VLANs, which receive multicast streams from the MVLAN. The MVR receiver ports comprise all the interfaces that exist on any of the MVR receiver VLANs. Interfaces that are on the MVLAN itself cannot be MVR receiver ports for that MVLAN.



NOTE: MVR is supported on VLANs running IGMP version 2 (IGMPv2) only.

MVR Modes

MVR operates in two modes: MVR transparent mode and MVR proxy mode. Both modes allow MVR to forward only one copy of a multicast stream to the Layer 2 network.

- MVR Transparent Mode on page 9
- MVR Proxy Mode on page 9

MVR Transparent Mode

In MVR transparent mode (the default mode), the switch receives one copy of each IPTV multicast stream and then replicates the stream only to those hosts that want to receive it, while forwarding all other types of multicast traffic without modification. Transparent mode is the default mode.

The switch handles IGMP packets destined for both the multicast source VLAN and multicast receiver VLANs in the same way that it handles them when MVR is not being used. That is, when a host on a VLAN sends IGMP join and leave messages, the switch floods the messages to all router interfaces in the VLAN. Similarly, when a VLAN receives IGMP queries from its router interfaces, it floods the queries to all interfaces in the VLAN.

If a host on a multicast receiver port joins an MVR group on the multicast receiver VLAN, the appropriate bridging entry is added and the MVLAN forwards that group's IPTV multicast traffic on that port (even though that port is not in the MVLAN). Likewise, if a host on a multicast receiver port leaves an MVR group on the multicast receiver VLAN, the appropriate bridging entry is deleted and the MVLAN stops forwarding that group's IPTV multicast traffic on that port. In addition, you can configure the switch to statically install the bridging entries on the multicast receiver VLAN.

MVR Proxy Mode

When you use MVR in proxy mode, the switch acts as a proxy for any MVR group in both the upstream and downstream directions. In the downstream direction, the switch acts as the querier for the groups in the MVR receiver VLANs. In the upstream direction, the switch originates the IGMP reports and leaves and answers IGMP queries from multicast routers. When the MVR receiver VLANs receive IGMP joins and leaves, the switch creates bridging entries on the MVLAN as needed, as it does in MVR transparent mode. In addition, the switch sends out IGMP joins and leaves on the MVLAN based on these bridging entries.

Configuring MVR proxy mode on the MVLAN automatically enables IGMP snooping proxy mode on all MVR receiver VLANs as well as on the MVLAN.

Related Topics

- Example: Configuring Multicast VLAN Registration on EX Series Switches on page 14
- Configuring Multicast VLAN Registration (CLI Procedure) on page 24

Chapter 2

Examples: IGMP Snooping and Multicast Configuration

- Example: Configuring IGMP Snooping on EX Series Switches on page 11
- Example: Configuring Multicast VLAN Registration on EX Series Switches on page 14

Example: Configuring IGMP Snooping on EX Series Switches

IGMP snooping regulates multicast traffic in a switched network. With IGMP snooping enabled, a LAN switch monitors the IGMP transmissions between a host (a network device) and a multicast router, keeping track of the multicast groups and associated member ports. The switch uses that information to make intelligent multicast-forwarding decisions and forward traffic to the intended destination interfaces.

Configure IGMP snooping on one or more VLANs to allow the switch to examine IGMP packets and make forwarding decisions based on packet content. By default, IGMP snooping is enabled on EX Series switches.

This example describes how to configure IGMP snooping:

- Requirements on page 11
- Overview and Topology on page 12
- Configuration on page 12

Requirements

This example uses the following software and hardware components:

- One EX3200-24T switch
- JUNOS Release 9.5 or later for EX Series switches

Before you configure IGMP snooping, be sure you have:

- Configured the `employee-vlan` VLAN on the switch
- Assigned interfaces `ge-0/0/1`, `ge-0/0/2`, and `ge-0/0/3` to `employee-vlan`

See Example: Setting Up Bridging with Multiple VLANs for EX Series Switches.

Overview and Topology

IGMP snooping controls multicast traffic in a switched network. With IGMP snooping enabled, an EX Series switch monitors the IGMP transmissions between a host and a multicast router to keep track of the multicast groups and associated member ports. The switch uses this information to make intelligent decisions and forward multicast traffic to the intended destination interfaces.

You can configure IGMP snooping on all interfaces in a VLAN or on individual interfaces. This example shows how to configure IGMP snooping on an EX Series switch.

The configuration setup for this example includes the VLAN `employee-vlan` on the switch.

Table 2 on page 12 shows the components of the topology for this example.

Table 2: Components of the IGMP Snooping Topology

Properties	Settings
Switch hardware	One EX3200-24T switch
VLAN name	<code>employee-vlan</code> , tag 20
Interfaces in <code>employee-vlan</code>	<code>ge-0/0/1</code> , <code>ge-0/0/2</code> , <code>ge-0/0/3</code>
Multicast IP address for <code>employee-vlan</code>	225.100.100.100

In this example, the switch is initially configured as follows:

- IGMP snooping is disabled on the VLAN.

Configuration

To configure basic IGMP snooping on a switch:

CLI Quick Configuration To quickly configure IGMP snooping, copy the following commands and paste them into the switch terminal window:

```
[edit protocols]
set igmp-snooping vlan employee-vlan
set igmp-snooping vlan employee-vlan interface ge-0/0/1 group-limit 50
set igmp-snooping vlan employee-vlan immediate-leave
set igmp-snooping vlan employee-vlan interface ge-0/0/3 static group
225.100.100.100
set igmp-snooping vlan employee-vlan interface ge-0/0/2 multicast-router-interface
set igmp-snooping vlan employee-vlan robust-count 4
```

Step-by-Step Procedure Configure IGMP snooping:

1. Enable and configure IGMP snooping on the VLAN employee-vlan:

```
[edit protocols]
user@switch# set igmp-snooping vlan employee-vlan
```

2. Configure the limit for the number of multicast groups allowed on the ge-0/0/1 interface to 50.

```
[edit protocols]
user@switch# set igmp-snooping vlan employee-vlan interface ge-0/0/1
group-limit 50
```

3. Configure the switch to immediately remove a group membership from an interface when it receives a leave message from that interface and suppress the sending of any group-specific queries for the multicast group (IGMPv2 only):

```
[edit protocols]
user@switch# set igmp-snooping vlan employee-vlan immediate-leave
```

4. Statically configure IGMP group membership on a port:

```
[edit protocols]
user@switch# set igmp-snooping vlan employee-vlan interface ge-0/0/3.0
static group 225.100.100.100
```

5. Statically configure an interface as a switching interface toward a multicast router (the interface to receive multicast traffic):

```
[edit protocols]
user@switch# set igmp-snooping vlan employee-vlan interface ge-0/0/2
multicast-router-interface
```

6. Change the number of timeout intervals the switch waits before timing out a multicast group to 4:

```
[edit protocols]
user@switch# set igmp-snooping vlan employee-vlan robust-count 4
```

Results Check the results of the configuration:

```
user@switch# show protocols igmp-snooping
vlan employee-vlan {
  robust-count 4;
  immediate-leave;
  interface ge-0/0/1 {
    group-limit 50;
  }
  interface ge-0/0/2 {
    multicast-router-interface;
  }
}
```

```

interface ge-0/0/3 {
  static {
    group 255.100.100.100
  }
}

```

- Related Topics**
- Configuring IGMP Snooping (CLI Procedure) on page 19
 - [edit protocols] Configuration Statement Hierarchy on page 31

Example: Configuring Multicast VLAN Registration on EX Series Switches

Multicast VLAN registration (MVR) allows hosts that are not part of a multicast VLAN (MVLAN) to receive multicast streams from the MVLAN, allowing the MVLAN to be shared across the Layer 2 network and eliminating the need to send duplicate multicast streams to each requesting VLAN in the network. Hosts remain in their own VLANs for bandwidth and security reasons.

This example describes how to configure MVR on EX Series switches:

- Requirements on page 14
- Overview and Topology on page 14
- Configuration on page 17

Requirements

This example uses the following hardware and software components:

- One EX Series switch
- JUNOS Release 9.6 or later for EX Series switches

Before you configure MVR, be sure you have:

- Configured two or more VLANs on the switch. See Example: Setting Up Bridging with Multiple VLANs for EX Series Switches.
- Connected the EX Series switch to a network that can transmit IPTV multicast streams from a video server.
- Connected a host that is capable of receiving IPTV multicast streams to an interface in one of the VLANs.

Overview and Topology

In a standard Layer 2 network, a multicast stream received on one VLAN is never distributed to interfaces outside that VLAN. If hosts in multiple VLANs request the same multicast stream, a separate copy of that multicast stream is distributed to the requesting VLANs.

MVR introduces the concept of a *multicast source VLAN* (MVLAN), which is created by MVR and becomes the only VLAN over which multicast traffic flows throughout the Layer 2 network. Multicast traffic can then be selectively forwarded from interfaces on the MVLAN (source ports) to hosts that are connected to interfaces (multicast receiver ports) that are not part of the multicast source VLAN. When you configure an MVLAN, you assign a range of multicast group addresses to it. You then configure other VLANs to be MVR receiver VLANs, which receive multicast streams from the MVLAN. The MVR receiver ports comprise all the interfaces that exist on any of the MVR receiver VLANs.

You can configure MVR to operate in one of two modes: transparent mode (the default mode) or proxy mode. Both modes allow MVR to forward only one copy of a multicast stream to the Layer 2 network.

In transparent mode, the switch receives one copy of each IPTV multicast stream and then replicates the stream only to those hosts that want to receive it, while forwarding all other types of multicast traffic without modification. Figure 1 shows how MVR operates in transparent mode.

In proxy mode, the switch acts as a proxy for the IGMP multicast router in the MVLAN for MVR group memberships established in the MVR receiver VLANs and generates and sends IGMP packets into the MVLAN as needed. Figure 2 shows how MVR operates in proxy mode.

This example shows how to configure MVR in both transparent mode and proxy mode on an EX Series switch. The topology includes a video server that is connected to a multicast router, which in turn forwards the IPTV multicast traffic in the MVLAN to the Layer 2 network.

Figure 3 on page 16 shows the MVR topology in transparent mode. Interfaces P1 and P2 on Switch C belong to service VLAN `s0` and MVLAN `mv0`. Interface P4 of Switch C also belongs to service VLAN `s0`. In the upstream direction of the network, only non-IPTV traffic is being carried in individual customer VLANs of service VLAN `s0`. VLAN `c0` is an example of this type of customer VLAN. IPTV traffic is being carried on MVLAN `mv0`. If any host on any customer VLAN connected to port P4 requests an MVR stream, switch C takes the stream from VLAN `mv0` and replicates that stream onto port P4 with tag `mv0`. IPTV traffic, along with other network traffic, flows from port P4 out to the Digital Subscriber Line Access Multiplexer (DSLAM) D1.

Figure 3: MVR Topology in Transparent Mode

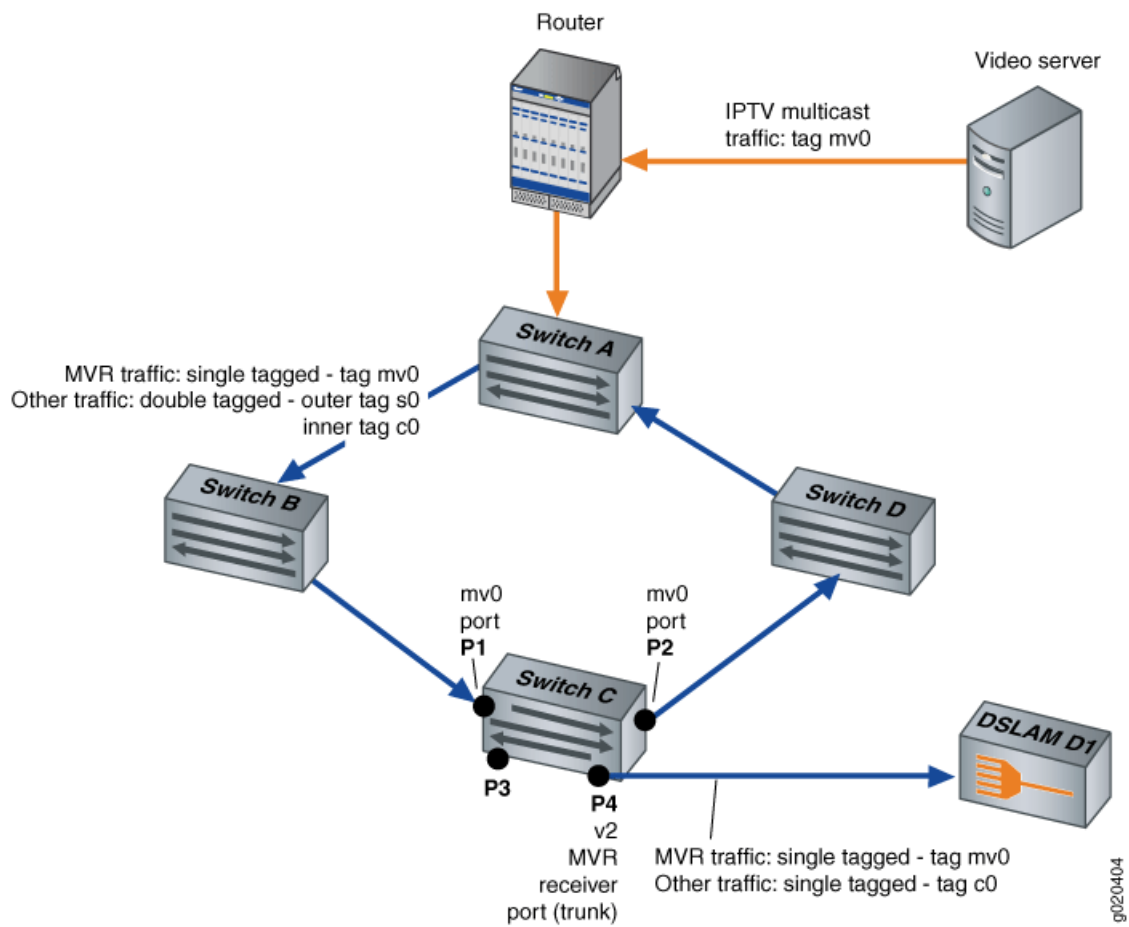
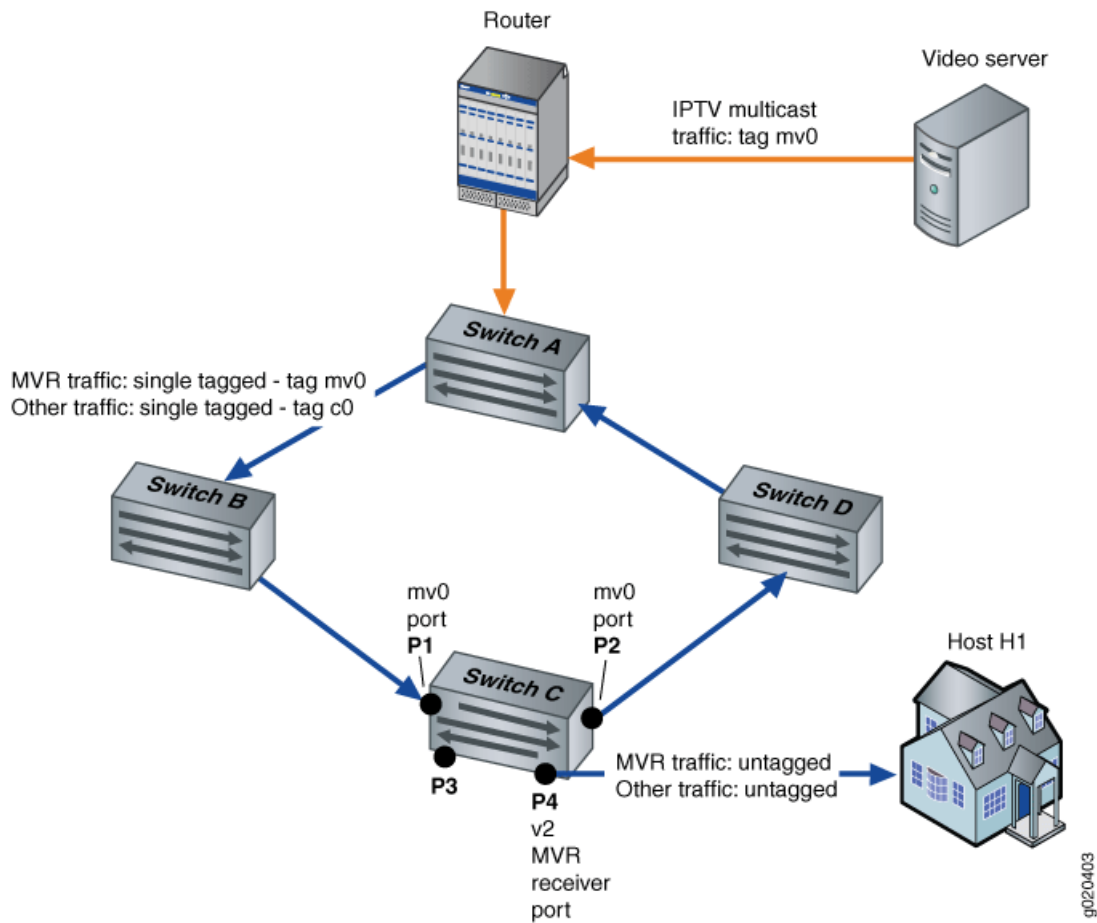


Figure 4 on page 17 shows the MVR topology in proxy mode. Interfaces P1 and P2 on switch C belong to MVLAN mv0 and customer VLAN c0. Interface P4 on switch C is an access port of customer VLAN c0. In the upstream direction of the network, only non-IPTV traffic is being carried on customer VLAN c0. Any IPTV traffic requested by hosts on VLAN c0 is replicated untagged to port P4 based on streams received in MVLAN mv0. IPTV traffic flows from port P4 out to an IPTV-enabled device in Host 1. Other traffic, such as data and voice traffic, also flows from port P4 to other network devices in Host 1.

Figure 4: MVR Topology in Proxy Mode

For information on VLAN tagging, see Understanding Bridging and VLANs on EX Series Switches.

Configuration

To configure MVR perform these tasks:

CLI Quick Configuration To quickly configure MVR in proxy mode, copy the following commands and paste them into the switch terminal window. To quickly configure MVR in transparent mode (the default mode), do not copy and paste the final command line in the following block of lines:

```
[edit protocols igmp-snooping]
set vlan mv0 data-forwarding source groups 225.10.0.0/16
set vlan v2 data-forwarding receiver source-vlans mv0
set vlan v2 data-forwarding receiver install
set vlan mv0 proxy source-address 10.1.1.1
```

Step-by-Step Procedure To configure MVR, perform these tasks:

1. Configure mv0 to be an MVLAN:

```
[edit protocols igmp-snooping]
user@switch# set vlan mv0 data-forwarding source groups 225.10.0.0/16
```

2. Configure v2 to be a multicast receiver VLAN with mv0 as its source:

```
[edit protocols igmp-snooping]
user@switch# set vlan v2 data-forwarding receiver source-vlans mv0
```

3. (Optional) Install forwarding entries in the multicast receiver VLAN v2:

```
[edit protocols igmp-snooping]
user@switch# set vlan v2 data-forwarding receiver install
```

4. (Optional) Configure MVR in proxy mode:

```
[edit protocols igmp-snooping]
user@switch# set vlan mv0 proxy source-address 10.1.1.1
```

Results Check the results of the configuration:

```
[edit protocols igmp-snooping]
user@switch# show
vlan mv0 {
  proxy {
    source-address 10.1.1.1;
  }
  data-forwarding {
    source {
      groups 225.10.0.0/16;
    }
  }
}
vlan v2 {
  data-forwarding {
    receiver {
      source-vlans mv0;
      install;
    }
  }
}
```

- Related Topics**
- Configuring Multicast VLAN Registration (CLI Procedure) on page 24
 - Understanding Multicast VLAN Registration on EX Series Switches on page 8

Chapter 3

Configuring IGMP Snooping and Multicast

- Configuring IGMP Snooping (CLI Procedure) on page 19
- Configuring IGMP Snooping (J-Web Procedure) on page 20
- Changing the IGMP Snooping Group Query Membership Timeout Value (CLI Procedure) on page 23
- Configuring Multicast VLAN Registration (CLI Procedure) on page 24

Configuring IGMP Snooping (CLI Procedure)

IGMP snooping regulates multicast traffic in a switched network. With IGMP snooping enabled, a LAN switch monitors the IGMP transmissions between a host (a network device) and a multicast router, keeping track of the multicast groups and associated member ports. The switch uses that information to make intelligent multicast-forwarding decisions and forward traffic to the intended destination interfaces.

You can configure IGMP snooping on one or more VLANs to allow the switch to examine IGMP packets and make forwarding decisions based on packet content. By default, IGMP snooping is enabled on EX Series switches.



NOTE: You cannot configure IGMP snooping on a secondary VLAN.

To enable IGMP snooping and configure individual options as needed for your network by using the CLI:

1. Enable IGMP snooping on a VLAN:

```
[edit protocols]
user@switch# set igmp-snooping vlan employee-vlan
```

2. Configure the limit for the number of multicast groups allowed on the `ge-0/0/1` interface to 50.

```
[edit protocols]
user@switch# set igmp-snooping vlan employee-vlan interface ge-0/0/1
group-limit 50
```

3. Configure the switch to immediately remove a multicast group membership from an interface when it receives a leave message from that interface and suppress the sending of any group-specific queries for the multicast group (IGMPv2 only):

```
[edit protocols]
user@switch# set igmp-snooping vlan employee-vlan immediate-leave
```

4. Statically configure IGMP group membership on a port:

```
[edit protocols]
user@switch# set igmp-snooping vlan employee-vlan interface ge-0/0/3.0
static group 225.100.100.100
```

5. Statically configure an interface as a switching interface toward a multicast router (the interface to receive multicast traffic):

```
[edit protocols]
user@switch# set igmp-snooping vlan employee-vlan interface ge-0/0/2.0
multicast-router-interface
```

6. Change the number of timeout intervals the switch waits before timing out a multicast group to 4:

```
[edit protocols]
user@switch# set igmp-snooping vlan employee-vlan robust-count 4
```

- Related Topics**
- Example: Configuring IGMP Snooping on EX Series Switches on page 11
 - Changing the IGMP Snooping Group Query Membership Timeout Value (CLI Procedure) on page 23
 - show igmp-snooping membership
 - show igmp-snooping route
 - show igmp-snooping statistics
 - show igmp-snooping vlans
 - IGMP Snooping on EX Series Switches Overview on page 3

Configuring IGMP Snooping (J-Web Procedure)

IGMP snooping regulates multicast traffic in a switched network. With IGMP snooping enabled, the EX Series switch monitors the IGMP transmissions between a host (a network device) and a multicast router, keeping track of the multicast groups and associated member interfaces. The switch uses that information to make intelligent multicast-forwarding decisions and forward traffic to the intended destination interfaces.

You can configure IGMP snooping on one or more VLANs to allow the switch to examine IGMP packets and make forwarding decisions based on packet content. By default, IGMP snooping is enabled on EX Series switches.

To enable IGMP snooping and configure individual options using the J-Web interface:

1. Select **Configure > Switching > IGMP Snooping**.
2. Click one:
 - **Add**—Creates an IGMP snooping configuration for the VLAN.
 - **Edit**—Modifies an IGMP snooping configuration for the VLAN.
 - **Delete**—Deletes a selected VLAN from the IGMP snooping configuration.

When you are adding or editing an IGMP snooping configuration, enter information as described in Table 3 on page 21

3. Click **OK** to apply changes to the configuration or click **Cancel** without saving changes.

To disable IGMP snooping on a VLAN, select the VLAN from the list and click **Disable**.

Table 3: IGMP Snooping Configuration Fields

Field	Function	Your Action
VLAN Name	Specifies the VLAN on which to enable IGMP snooping.	Select a VLAN from the list to add it to the snooping configuration.
Immediate Leave	Immediately removes a multicast group membership from an interface when it receives a leave message from that interface and suppresses the sending of any group-specific queries for the multicast group	To enable the option, select the check box. To disable the option, clear the check box.
Robust Count	Specifies the number of timeout intervals the switch waits before timing out a multicast group.	Type a value.

Table 3: IGMP Snooping Configuration Fields (continued)

Field	Function	Your Action
Interfaces List	Statically configures an interface as a switching interface toward a multicast router (the interface to receive multicast traffic).	<p>Click one:</p> <ul style="list-style-type: none"> ■ Add—Adds an interface to the IGMP snooping configuration. <ol style="list-style-type: none"> 1. Select an interface from the list. 2. Select Multicast Router Interface. 3. Type the maximum number of groups an interface can join. 4. In Static, choose one: <ul style="list-style-type: none"> ■ Click Add, type a group IP address, and click OK. ■ Select a group and click Remove to remove the group membership. ■ Edit—Edits the interface settings for the IGMP snooping configuration. ■ Remove—Deletes an interface configured for IGMP snooping.

- Related Topics**
- Example: Configuring IGMP Snooping on EX Series Switches on page 11
 - Configuring IGMP Snooping (CLI Procedure) on page 19
 - Changing the IGMP Snooping Group Query Membership Timeout Value (CLI Procedure) on page 23
 - IGMP Snooping on EX Series Switches Overview on page 3

Changing the IGMP Snooping Group Query Membership Timeout Value (CLI Procedure)

Generally, you do not need to explicitly set the group membership timeout value for IGMP snooping groups on an EX Series switch. The group membership timeout value, which determines how long the switch waits before removing an IGMP snooping group from its multicast cache table, is implicitly set to 260 seconds when you configure IGMP snooping.

When you enable IGMP snooping on a switch, the `query-interval` and `query-response-interval` values are set to their default values and are applied to all VLANs created on the switch. The default values are:

- `query-interval`—125 seconds
- `query-response-interval`—10 seconds

The software automatically calculates the group membership timeout value for an IGMP snooping-enabled switch by multiplying the `query-interval` value by 2 and then adding the `query-response-interval` value. For example, using the default values: $(125 \times 2) + 10 = 260$.

If you need to explicitly set the group membership timeout value, you reset the `query-interval` and `query-response-interval` values at the `[edit protocols igmp]` hierarchy level. (Notice that you are not resetting the values at the `[edit protocols igmp-snooping]` hierarchy level.) When you reset these values, the IGMP snooping configuration inherits the new values and recalculates the group membership timeout value accordingly. For more information on changing these values, see the *JUNOS Multicast Protocols Configuration Guide* at <http://www.juniper.net/techpubs/software/junos/junos96/index.html>.

To change the IGMP snooping group membership timeout value to 350:

1. Configure the `query-interval` value to be 150:

```
[edit protocols]
user@switch# set igmp query-interval 150
```

2. Configure the `query-response-interval` value to be 50:

```
[edit protocols]
user@switch# set igmp query-response-interval 50
```

- Related Topics**
- Example: Configuring IGMP Snooping on EX Series Switches on page 11
 - Verifying That the IGMP Snooping Group Query Timeout Value Has Been Changed Correctly on page 28
 - Configuring IGMP Snooping (CLI Procedure) on page 19
 - Configuring IGMP Snooping (J-Web Procedure) on page 20

Configuring Multicast VLAN Registration (CLI Procedure)

Multicast VLAN registration (MVR) allows hosts that are not part of a multicast source VLAN (MVLAN) to still receive multicast streams from the MVLAN, allowing an MVLAN to be shared across a Layer 2 network. Hosts remain in their own VLANs for bandwidth and security reasons but are able to receive multicast streams from the MVLAN.

You can configure one or more VLANs on a switch to be MVLANS or MVR receiver VLANs. By default, MVR is not configured on EX Series switches.



NOTE: MVR is supported on VLANs running IGMP version 2 (IGMPv2) only.



NOTE: When configuring MVR, the following restrictions apply:

- You cannot enable multicast protocols on VLAN interfaces that are members of MVLANS.
 - If you configure an MVLAN in proxy mode, IGMP snooping proxy mode will be automatically enabled on all MVR receiver VLANs of this MVLAN. If a VLAN is an MVR receiver VLAN for multiple MVLANS, all of the MVLANS must have proxy mode enabled or all must have proxy mode disabled. You can enable proxy mode only on VLANs that are configured as MVR source VLANs and that are not configured for Q-in-Q tunneling.
 - After you configure a VLAN as an MVLAN, that VLAN is no longer available for other uses.
-

To configure MVR:

1. Configure the VLAN named `mv0` to be an MVLAN:

```
[edit protocols]
user@switch# set igmp-snooping vlan mv0 data-forwarding source groups
225.10.0.0/16
```

2. Configure the MVLAN `mv0` to be a proxy VLAN:

```
[edit protocols]
user@switch# set igmp-snooping vlan mv0 proxy source-address 10.0.0.1
```

3. Configure the VLAN named `v2` to be an MVR receiver VLAN:

```
[edit protocols]
user@switch# set igmp-snooping vlan v2 data-forwarding receiver source-vlans
mv0
```

4. Install forwarding entries in the MVR receiver VLAN:

```
[edit protocols]  
user@switch# set igmp-snooping vlan mv0 data-forwarding receiver install
```

- Related Topics**
- Example: Configuring Multicast VLAN Registration on EX Series Switches on page 14
 - Understanding Multicast VLAN Registration on EX Series Switches on page 8

Chapter 4

Verifying IGMP Snooping and Multicast

- Monitoring IGMP Snooping on page 27
- Verifying That the IGMP Snooping Group Query Timeout Value Has Been Changed Correctly on page 28

Monitoring IGMP Snooping

Purpose Use the monitoring feature to view status and information about IGMP snooping configuration on your EX Series switch.

Action To display IGMP snooping details in the J-Web interface, select Monitor > Switching > IGMP Snooping.

To display IGMP snooping details in the CLI, enter the following commands:

- `show igmp-snooping vlans`
- `show igmp-snooping statistics`
- `show igmp-snooping route`

Meaning Table 4 on page 27 summarizes the IGMP snooping details displayed.

Table 4: Summary of IGMP Snooping Output Fields

Field	Values
IGMP Snooping Monitor	
VLAN	The VLAN for which IGMP snooping is enabled.
Interfaces	Indicates the interfaces configured as switching interfaces that are associated with the multicast router.
Groups	Indicates the number of the multicast groups learned by the VLAN.
MRouters	Specifies the multicast router.
Receivers	Specifies the multicast receiver.
IGMP Route Information	
VLAN	The VLAN for which IGMP snooping is enabled.

Table 4: Summary of IGMP Snooping Output Fields (continued)

Field	Values
Next-Hop	Specifies the next hop assigned by the switch after performing the route lookup.
Group	Indicates the multicast groups learned by the VLAN.

- Related Topics**
- `show igmp-snooping vlans`
 - `show igmp-snooping statistics`
 - `show igmp-snooping route`
 - Configuring IGMP Snooping (CLI Procedure) on page 19
 - Example: Configuring IGMP Snooping on EX Series Switches on page 11

Verifying That the IGMP Snooping Group Query Timeout Value Has Been Changed Correctly

Purpose Verify that the IGMP snooping group query timeout value has been changed correctly from its default value.

Action Display the IGMP protocol information:

```
user@switch> show configuration protocols igmp
query-interval 150;
query-response-interval 50;
accounting;
interface vlan.43 {
    version 2;
}
```

Display the IGMP snooping membership information, which contains the group query timeout value that was derived from the IGMP configuration:

```
user@switch> show show igmp-snooping membership detail
VLAN: v43 Tag: 43 (Index: 4)
Group: 225.0.0.1
Receiver count: 1, Flags: <v2-hosts>
ge-0/0/15.0 Uptime: 00:00:05 timeout: 350
```

Meaning When you enable IGMP snooping on a switch, the `query-interval` and `query-response-interval` values are set to their default values and are applied to all VLANs created on the switch. The IGMP snooping group timeout value is derived from these default settings. Based on the default values, the initial IGMP snooping group query timeout value is 260.

To change the group query timeout value, change the `query-interval` and `query-response-interval` values at the `[edit protocols igmp]` hierarchy level. The IGMP snooping group query timeout value is then recalculated based on the new IGMP configuration settings.

The output from the `show protocols igmp` command shows the revised IGMP configuration settings for `query-interval` and `query-response-interval`. You know that these values have been revised because they are different from the default values. The output from the `show igmp-snooping membership detail` command shows the revised group query timeout value, 350, which was derived from the new IGMP configuration settings.

- Related Topics**
- Changing the IGMP Snooping Group Query Membership Timeout Value (CLI Procedure) on page 23

Chapter 5

Configuration Statements for IGMP Snooping and Multicast

- [edit protocols] Configuration Statement Hierarchy on page 31

[edit protocols] Configuration Statement Hierarchy

```
protocols {
  connections {
    remote-interface-switch connection-name {
      interface interface-name.unit-number;
      transmit-lsp label-switched-path;
      receive-lsp label-switched-path;
    }
  }
  dot1x {
    authenticator {
      authentication-profile-name profile-name;
      interface (all | [ interface-names ]) {
        disable;
        guest-vlan ( vlan-id | vlan-name );
        mac-radius <restrict>;
        maximum-requests number;
        no-reauthentication;
        quiet-period seconds;
        reauthentication {
          interval seconds;
        }
        retries number;
        server-fail (deny | permit | use-cache | vlan-id | vlan-name);
        server-reject-vlan ( vlan-id | vlan-name );
        server-timeout seconds;
        supplicant (multiple | single | single-secure);
        supplicant-timeout seconds;
        transmit-period seconds;
      }
    }
    static mac-address {
      interface interface-name;
      vlan-assignment ( vlan-id | vlan-name );
    }
  }
  gvrp {
    <enable | disable>;
  }
}
```

```

interface (all | [interface-name]) {
  disable;
}
join-timer milliseconds;
leave-timer milliseconds;
leaveall-timer milliseconds;
}
igmp-snooping {
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>
    <match regex>;
    flag flag (detail | disable | receive | send);
  }
  vlan (vlan-id | vlan-number) {
    data-forwarding {
      source {
        groups group-prefix;
      }
      receiver {
        source-vlans vlan-list;
        install ;
      }
    }
  }
  disable {
    interface interface-name
  }
  immediate-leave;
  interface interface-name {
    group-limit limit;
    multicast-router-interface;
    static {
      group ip-address;
    }
  }
  proxy ;
  query-interval seconds;
  query-last-member-interval seconds;
  query-response-interval seconds;
  robust-count number;
}
}
lldp {
  disable;
  advertisement-interval seconds;
  hold-multiplier number;
  interface (all | interface-name) {
    disable;
  }
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>
    <match regex>;
    flag flag (detail | disable | receive | send);
  }
}
}
lldp-med {
  disable;
}

```

```

fast-start number;
interface (all | interface-name) {
  disable;
  location {
    elin number;
    civic-based {
      what number;
      country-code code;
      ca-type {
        number {
          ca-value value;
        }
      }
    }
  }
}
}
mpls {
  interface ( all | interface-name );
  label-switched-path lsp-name to remote-provider-edge-switch;
  path destination {
    <address | hostname> <strict | loose>
  }
}
mstp {
  disable;
  bpdu-block-on-edge;
  bridge-priority priority;
  configuration-name name;
  forward-delay seconds;
  hello-time seconds;
  interface (all | interface-name) {
    disable;
    bpdu-timeout-action {
      block;
      alarm;
    }
    cost cost;
    edge;
    mode mode;
    no-root-port;
    priority priority;
  }
  max-age seconds;
  max-hops hops;
  msti msti-id {
    vlan (vlan-id | vlan-name);
    interface interface-name {
      disable;
      cost cost;
      edge;
      mode mode;
      priority priority;
    }
  }
  revision-level revision-level;
  traceoptions {

```

```

        file filename <files number > <size size> <no-stamp | world-readable |
          no-world-readable>;
        flag flag;
    }
}
mvrp {
    disable
    interface (all | interface-name) {
        disable;
        join-timer milliseconds;
        leave-timer milliseconds;
        leaveall-timer milliseconds;
        registration (forbidden | normal);
    }
    no-dynamic-vlan;
    traceoptions {
        file filename <files number > <size size> <no-stamp | world-readable |
          no-world-readable>;
        flag flag;
    }
}
oam {
    ethernet{
        link-fault-management {
            action-profile profile-name;
            action {
                syslog;
                link-down;
            }
            event {
                link-adjacency-loss;
                link-event-rate;
                frame-error count;
                frame-period count;
                frame-period-summary count;
                symbol-period count;
            }
            interface interface-name {
                link-discovery (active | passive);
                pdu-interval interval;
                event-thresholds threshold-value;
                remote-loopback;
                event-thresholds {
                    frame-error count;
                    frame-period count;
                    frame-period-summary count;
                    symbol-period count;
                }
            }
            negotiation-options {
                allow-remote-loopback;
                no-allow-link-events;
            }
        }
    }
}
rstp {

```

```

disable;
bpdu-block-on-edge;
bridge-priority priority;
forward-delay seconds;
hello-time seconds;
interface (all | interface-name) {
    disable;
    bpdu-timeout-action {
        block;
        alarm;
    }
    cost cost;
    edge;
    mode mode;
    no-root-port;
    priority priority;
}
max-age seconds;
}
traceoptions {
    file filename <files number > <size size> <no-stamp | world-readable |
    no-world-readable>;
    flag flag;
}
}
sflow {
    collector {
        ip-address;
        udp-port port-number;
    }
    disable;
    interfaces interface-name {
        disable;
        polling-interval seconds;
        sample-rate number;
    }
    polling-interval seconds;
    sample-rate number;
}
stp {
    disable;
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
        disable;
        bpdu-timeout-action {
            block;
            alarm;
        }
        cost cost;
        edge;
        mode mode;
        no-root-port;
        priority priority;
    }
}

```

```

    max-age seconds;
  }
  traceoptions {
    file filename <files number > <size size> <no-stamp | world-readable |
      no-world-readable>;
    flag flag;
  }
  vstp {
    bpdu-block-on-edge;
    disable;
    force-version stp;
    vlan (all | vlan-id | vlan-name) {
      bridge-priority priority;
      forward-delay seconds;
      hello-time seconds;
      interface (all | interface-name) {
        bpdu-timeout-action {
          alarm;
          block;
        }
        cost cost;
        disable;
        edge;
        mode mode;
        no-root-port;
        priority priority;
      }
      max-age seconds;
      traceoptions {
        file filename <files number > <size size> <no-stamp | world-readable |
          no-world-readable>;
        flag flag;
      }
    }
  }
}

```

- Related Topics**
- 802.1X for EX Series Switches Overview
 - Example: Configure Automatic VLAN Administration Using GVRP
 - Understanding MAC RADIUS Authentication on EX Series Switches
 - Understanding Server Fail Fallback and 802.1X Authentication on EX Series Switches
 - IGMP Snooping on EX Series Switches Overview on page 3
 - Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches
 - Understanding MSTP for EX Series Switches
 - Understanding RSTP for EX Series Switches
 - Understanding STP for EX Series Switches
 - Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch

- Understanding VSTP for EX Series Switches
- Understanding Ethernet OAM Link Fault Management for an EX Series Switch

data-forwarding

Syntax data-forwarding {
 source {
 groups *group-prefix*;
 }
 receiver {
 source-vlans *vlan-list*;
 install;
 }
 }

Hierarchy Level [edit protocols igmp-snooping vlan *vlan-id* | *vlan-number*]

Release Information Statement introduced in JUNOS Release 9.6 for EX Series switches.

Description Configure the VLAN to be a multicast source VLAN (MVLAN) or a multicast VLAN registration (MVR) receiver VLAN. Each data-forwarding VLAN, which can be a multicast source VLAN (MVLAN) or a multicast receiver VLAN, must have exactly one source statement or exactly one receiver statement. A data-forwarding VLAN can operate only in IGMPv2 mode.

The remaining statements are explained separately.

Default Disabled.

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

- Related Topics**
- [edit protocols] Configuration Statement Hierarchy on page 31
 - Example: Configuring Multicast VLAN Registration on EX Series Switches on page 14
 - Configuring Multicast VLAN Registration (CLI Procedure) on page 24

disable

Syntax	disable { interface <i>interface-name</i> }
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-name</i>]
Release Information	Statement introduced in JUNOS Release 9.2 for EX Series switches.
Description	Disable IGMP snooping on all interfaces in a VLAN or on a specific VLAN interface.
Default	If you do not specify an interface, all interfaces in the given VLAN are disabled.
Options	<i>interface-name</i> —Name of the interface.
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 IGMP Snooping on EX Series Switches on page 11 ■ Configuring IGMP Snooping (CLI Procedure) on page 19

group

Syntax	group <i>ip-address</i> ;
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-name</i> interface <i>interface-name</i> static]
Release Information	Statement introduced in JUNOS Release 9.1 for EX Series switches.
Description	Configure a static multicast group using a valid IP multicast address.
Default	None.
Options	<i>ip-address</i> —IP address of the multicast group receiving data on an interface.
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 IGMP Snooping on EX Series Switches on page 11 ■ Configuring IGMP Snooping (CLI Procedure) on page 19

groups

Syntax	<code>groups group-prefix;</code>
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-number</i> data-forwarding source]
Release Information	Statement introduced in JUNOS Release 9.6 for EX Series switches.
Description	Specify the IP address range of the multicast VLAN (MVLAN) source interfaces.
Default	Disabled.
Options	<i>group-prefix</i> —IP address range of the source group. Each MVLAN must have exactly one groups statement. If there are multiple MVLANS on the switch, their group ranges must be unique.
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"> ■ [edit protocols] Configuration Statement Hierarchy on page 31 ■ Example: Configuring Multicast VLAN Registration on EX Series Switches on page 14 ■ Configuring Multicast VLAN Registration (CLI Procedure) on page 24

group-limit

Syntax	<code>group-limit <i>limit</i>;</code>
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-number</i> interface <i>interface-name</i>]
Release Information	Statement introduced in JUNOS Release 9.5 for EX Series switches.
Description	Configure a limit for the number of multicast groups allowed on the specified interface. After this limit is reached, new reports are ignored and related flows are not flooded on the interface.
Default	No group limits are configured.
Options	<p><i>limit</i> —Number that represents the maximum number of multicast groups allowed on the specified interface.</p> <p>Range: 0 through 65535</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 IGMP Snooping on EX Series Switches on page 11 ■ Configuring IGMP Snooping (CLI Procedure) on page 19 ■ Configuring IGMP Snooping (J-Web Procedure) on page 20 ■ <code>group</code>

igmp-snooping

```

Syntax  igmp-snooping {
            traceoptions {
                file filename <files number> <size size> <world-readable | no-world-readable> <match
                    regex>;
                flag flag (detail | disable | receive | send);
            }
            vlan vlan-id | vlan-name {
                data-forwarding {
                    source {
                        groups group-prefix;
                    }
                    receiver {
                        source-vlans vlan-list;
                        install ;
                    }
                }
            }
            disable {
                interface interface-name;
            }
            immediate-leave;
            interface interface-name {
                group-limit limit;
                multicast-router-interface;
                static {
                    group ip-address;
                }
            }
            proxy ;
            query-interval seconds;
            query-last-member-interval seconds;
            query-response-interval seconds;
            robust-count number;
        }
    
```

Hierarchy Level [edit protocols]

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

Description Enable and configure IGMP snooping on EX Series switches.

The remaining statements are explained separately.

Default IGMP snooping is enabled by default.

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

- Related Topics**
- Example: Configuring IGMP Snooping on EX Series Switches on page 11
 - Configuring IGMP Snooping (CLI Procedure) on page 19

immediate-leave

Syntax immediate-leave;

Hierarchy Level [edit protocols igmp-snooping vlan *vlan-id* | *vlan-name*]

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

Description (Applies only to switches running IGMPv2.) After the switch receives a leave group membership message from a host, immediately remove the group membership from the interface and suppress the sending of any group-specific queries for the multicast group.



NOTE: When configuring this statement, ensure that the IGMP interface has only one IGMP host connected. If more than one IGMPv2 host is connected to the switch through the same interface and one of the hosts sends a leave message, the switch removes all hosts on the interface from the multicast group. The switch loses contact with the hosts in the multicast group that did not send a leave message until they send join requests in response to the next general multicast listener query from the router.

Default The immediate-leave feature is disabled.

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

Related Topics

- Example: Configuring IGMP Snooping on EX Series Switches on page 11
- Configuring IGMP Snooping (CLI Procedure) on page 19

install

Syntax	install;
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-number</i> data-forwarding receiver]
Release Information	Statement introduced in JUNOS Release 9.6 for EX Series switches.
Description	Install forwarding entries in the multicast receiver VLAN. By default, only the multicast VLAN (MVLAN) installs forwarding entries for MVLAN groups.
Default	Disabled.
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">■ [edit protocols] Configuration Statement Hierarchy on page 31■ Example: Configuring Multicast VLAN Registration on EX Series Switches on page 14■ Configuring Multicast VLAN Registration (CLI Procedure) on page 24

interface

Syntax `interface interface-name {
 group-limit limit;
 multicast-router-interface;
 static {
 group ip-address;
 }
 }`

Hierarchy Level [edit protocols igmp-snooping vlan *vlan-id* | *vlan-name*]

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

Description Enable IGMP snooping on an interface and configure interface-specific properties.

The remaining statements are explained separately.

Default None.

Options *interface-name*—Name of the interface.

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

- Related Topics**
- show igmp-snooping vlans
 - Example: Configuring IGMP Snooping on EX Series Switches on page 11
 - Configuring IGMP Snooping (CLI Procedure) on page 19

multicast-router-interface

Syntax `multicast-router-interface;`

Hierarchy Level [edit protocols igmp-snooping vlan *vlan-id* | *vlan-name* interface *interface-name*]

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

Description Statically configure an interface as a switching interface toward a multicast router (the interface to receive multicast traffic).

Default Disabled.

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

- Related Topics**
- Example: Configuring IGMP Snooping on EX Series Switches on page 11
 - Configuring IGMP Snooping (CLI Procedure) on page 19

proxy

Syntax	<code>proxy source-address <i>source-address</i>;</code>
Hierarchy Level	<code>[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-number</i>]</code>
Release Information	Statement introduced in JUNOS Release 9.6 for EX Series switches.
Description	Specify that the VLAN operates in proxy mode. The proxy option is only accepted for a VLAN acting as a data-forwarding source.
Default	Disabled.
Options	<code>source-address <i>source-address</i></code> —IP address of the source VLAN to act as proxy.
Required Privilege Level	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ [edit protocols] Configuration Statement Hierarchy on page 31 ■ Example: Configuring Multicast VLAN Registration on EX Series Switches on page 14 ■ Configuring Multicast VLAN Registration (CLI Procedure) on page 24

query-interval

Syntax query-interval *seconds*;

Hierarchy Level [edit protocols igmp-snooping vlan *vlan-id* | *vlan-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: This statement has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use.

Description Configure how frequently the switch sends host-query timeout messages to a multicast group.

Default 125 seconds.

Options *seconds*—Number of seconds between host-query timeout messages.
Range: 1 through 1024 seconds

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

Related Topics

- Example: Configuring IGMP Snooping on EX Series Switches on page 11
- Configuring IGMP Snooping (CLI Procedure) on page 19

query-last-member-interval

Syntax query-last-member-interval *seconds*;

Hierarchy Level [edit protocols igmp-snooping vlan *vlan-id* | *vlan-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: This statement has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use.

Description Configure the interval between group-specific query timeout messages sent by the switch.

Default 1 second.

Options *seconds*—Amount of time between group-specific query timeout messages.
Range: 1 through 1024 seconds

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

Related Topics

- Example: Configuring IGMP Snooping on EX Series Switches on page 11
- Configuring IGMP Snooping (CLI Procedure) on page 19

query-response-interval

Syntax query-response-interval *seconds*;

Hierarchy Level [edit protocols igmp-snooping vlan *vlan-id* | *vlan-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: This statement has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use.

Description Configure the length of time the switch waits to receive a response to a specific query message from a host.

Default 10 seconds.

Options *seconds* —Number of seconds the switch waits to receive a response to a specific query message from a host.
Range: 1 through 25 seconds

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

Related Topics

- Example: Configuring IGMP Snooping on EX Series Switches on page 11
- Configuring IGMP Snooping (CLI Procedure) on page 19

receiver

Syntax	receiver { source-vlans <i>vlan-list</i> ; install; }
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-number</i> data-forwarding]
Release Information	Statement introduced in JUNOS Release 9.6 for EX Series switches.
Description	Configure a VLAN as a multicast receiver VLAN of the multicast VLAN (MVLAN). The remaining statements are explained separately.
Default	Disabled.
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"> ■ [edit protocols] Configuration Statement Hierarchy on page 31 ■ Example: Configuring Multicast VLAN Registration on EX Series Switches on page 14 ■ Configuring Multicast VLAN Registration (CLI Procedure) on page 24

robust-count

Syntax	robust-count <i>number</i> ;
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-name</i>]
Release Information	Statement introduced in JUNOS Release 9.1 for EX Series switches.
Description	Configure the number of intervals the switch waits before removing a multicast group from the multicast forwarding table. The length of each interval is configured using the <code>query-interval</code> statement.
Default	2
Options	<i>number</i> —Number of intervals the switch waits before timing out a multicast group. Range: 2 through 10
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 IGMP Snooping on EX Series Switches on page 11 ■ Configuring IGMP Snooping (CLI Procedure) on page 19

source

Syntax	source { groups <i>group-prefix</i> ; }
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-number</i> data-forwarding]
Release Information	Statement introduced in JUNOS Release 9.6 for EX Series switches.
Description	Configure a VLAN to be a multicast source VLAN (MVLAN). The remaining statement is explained separately.
Default	Disabled.
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"> ■ [edit protocols] Configuration Statement Hierarchy on page 31 ■ Example: Configuring Multicast VLAN Registration on EX Series Switches on page 14 ■ Configuring Multicast VLAN Registration (CLI Procedure) on page 24

source-vlans

Syntax	source-vlans <i>vlan-list</i> ;
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-number</i> data-forwarding receiver]
Release Information	Statement introduced in JUNOS Release 9.6 for EX Series switches.
Description	Specify a list of multicast VLANs (MVLANS) from which this multicast receiver VLAN receives multicast traffic. Either all of these MVLANS must be in proxy mode or none of them can be in proxy mode.
Default	Disabled.
Options	<i>vlan-list</i> —Names of the MVLANS.
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"> ■ [edit protocols] Configuration Statement Hierarchy on page 31 ■ Example: Configuring Multicast VLAN Registration on EX Series Switches on page 14 ■ Configuring Multicast VLAN Registration (CLI Procedure) on page 24

traceoptions

Syntax traceoptions {
 file *filename* <files *number*> <size *size*> <world-readable | no-world-readable> <match
 regex>;
 flag *flag* (detail | disable | receive | send);
 }

Hierarchy Level [edit protocols igmp-snooping]

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

Description Define tracing operations for IGMP snooping.

Default The traceoptions feature is disabled by default.

Options file *filename* —Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`.

files *number* —(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached (`xk` to specify KB, `xm` to specify MB, or `xg` to specify gigabytes), at which point the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the `size` option.

Range: 2 through 1000

Default: 3 files

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

- all—All tracing operations.
- general—Trace general IGMP snooping protocol events.
- leave—Trace leave group messages (IGMPv2 only).
- normal—Trace normal IGMP snooping protocol events.
- packets—Trace all IGMP packets.
- policy—Trace policy processing.
- query—Trace IGMP membership query messages.
- report—Trace membership report messages.
- route—Trace routing information.
- state—Trace IGMP state transitions.
- task—Trace routing protocol task processing.
- timer—Trace routing protocol timer processing.

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

no-world-readable—(Optional) Restricted file access to the user who created the file.

size *size* —(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the **files** option.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify gigabytes

Range: 10 KB through 1 gigabytes

Default: 128 KB

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

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

- Related Topics**
- Example: Configuring IGMP Snooping on EX Series Switches on page 11
 - Configuring IGMP Snooping (CLI Procedure) on page 19

vlan

Syntax `vlan (vlan-id | vlan-name) {`
 `data-forwarding {`
 `source {`
 `groups group-prefix;`
 `}`
 `receiver {`
 `source-vlans vlan-list;`
 `install ;`
 `}`
 `}`
 `disable {`
 `interface interface-name;`
 `}`
 `immediate-leave;`
 `interface interface-name {`
 `group-limit limit;`
 `multicast-router-interface;`
 `static {`
 `group ip-address;`
 `}`
 `}`
 `proxy ;`
 `query-interval seconds;`
 `query-last-member-interval seconds;`
 `query-response-interval seconds;`
 `robust-count number;`
 `}`

Hierarchy Level [edit protocols igmp-snooping]

Release Information Statement introduced in JUNOS Release 9.1 for EX Series switches.
 Statement updated with enhanced ? (CLI completion feature) functionality in JUNOS Release 9.5 for EX Series switches.

Description Configure IGMP snooping parameters for a VLAN.

The remaining statements are 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. For IGMP snooping, secondary private VLANs are not listed.

Default IGMP snooping options apply to the specified VLAN.

Options `vlan-id`—Numeric tag for a VLAN.

Range: 0 through 4095. Tags 0 and 4095 are reserved by JUNOS Software, and you should not configure them.

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**
- Configuring IGMP Snooping (CLI Procedure) on page 19
 - IGMP Snooping on EX Series Switches Overview on page 3

Chapter 6

Operational Mode Commands for IGMP Snooping and Multicast

clear igmp-snooping membership

Syntax	clear igmp-snooping membership <vlan <i>vlan-id</i> <i>vlan-name</i> >
Release Information	Command introduced in JUNOS Release 9.1 for EX Series switches.
Description	Clear IGMP snooping membership information.
Options	vlan <i>vlan-id</i> —Numeric tag identifier of the VLAN. vlan <i>vlan-name</i> —Name of the VLAN.
Required Privilege Level	view
Related Topics	■ show igmp-snooping membership
List of Sample Output	clear igmp-snooping membership on page 56
clear igmp-snooping membership	user@switch> clear igmp-snooping membership vlan employee-vlan

clear igmp-snooping statistics

Syntax	clear igmp-snooping statistics
Release Information	Command introduced in JUNOS Release 9.1 for EX Series switches.
Description	Clear IGMP snooping statistics.
Required Privilege Level	view
Related Topics	■ show igmp-snooping statistics
List of Sample Output	clear igmp-snooping statistics on page 57
clear igmp-snooping statistics	user@switch> clear igmp-snooping statistics

show igmp-snooping membership

- Syntax** show igmp-snooping membership
 <brief | detail>
 <interface *interface-name*>
 <vlan *vlan-id* | *vlan-name*>
- Release Information** Command introduced in JUNOS Release 9.1 for EX Series switches.
- Description** Display IGMP snooping membership information.
- Options** none—Display general parameters.
- brief | detail—(Optional) Display the specified level of output.
- interface *interface-name*—(Optional) Display IGMP snooping information for the specified interface.
- vlan *vlan-id* | *vlan-name*—(Optional) Display IGMP snooping information for the specified VLAN.
- Required Privilege Level** view
- Related Topics**
- show igmp-snooping route
 - show igmp-snooping statistics
 - show igmp-snooping vlans
 - Monitoring IGMP Snooping on page 27
 - Configuring IGMP Snooping (CLI Procedure) on page 19
 - Configuring IGMP Snooping (J-Web Procedure) on page 20
- List of Sample Output** show igmp-snooping membership on page 59
 show igmp-snooping membership detail on page 60
- Output Fields** Table 5 on page 58 lists the output fields for the show igmp-snooping membership command. Output fields are listed in the approximate order in which they appear.

Table 5: show igmp-snooping membership Output Fields

Field Name	Field Description	Level of Output
VLAN	Name of the VLAN.	All
Interfaces	Interfaces assigned to the VLAN.	All
Tag	Numerical identifier of the VLAN.	detail

Table 5: show igmp-snooping membership Output Fields (continued)

Field Name	Field Description	Level of Output
Router interfaces	Names multicast router interfaces.	detail
■ static or dynamic	Whether the multicast router interface is static or dynamic .	detail
■ Uptime	For static interfaces, amount of time since the interface was configured as a multicast router interface; for dynamic interfaces, amount of time since the first query was received on interface.	detail
■ timeout	Query timeout in seconds.	detail
Group	IP multicast address of the multicast group.	detail
Receiver count	Number of interfaces that have membership in a multicast group.	detail
Flags	IGMP version of the host sending a join message.	detail
Uptime	Amount of time a multicast group has been active on the interface.	detail
timeout	Time (in seconds) left until the entry for the multicast group is removed.	All
Last reporter	The last host to report membership for the multicast group.	detail
Include source	Source addresses from which multicast streams are allowed based on IGMPv3 reports.	detail

```

show igmp-snooping membership user@switch> show igmp-snooping membership
VLAN: v1
  224.1.1.1      *           258 secs
    Interfaces: ge-0/0/0.0
  224.1.1.3      *           258 secs
    Interfaces: ge-0/0/0.0
  224.1.1.5      *           258 secs
    Interfaces: ge-0/0/0.0
  224.1.1.7      *           258 secs
    Interfaces: ge-0/0/0.0
  224.1.1.9      *           258 secs
    Interfaces: ge-0/0/0.0
  224.1.1.11     *           258 secs
    Interfaces: ge-0/0/0.0

```

```
show igmp-snooping membership detail user@switch> show igmp-snooping membership detail
membership detail
VLAN: v43 Tag: 43 (Index: 4)
  Group: 225.0.0.2
  Receiver count: 1, Flags: <V3-hosts>
    ge-0/0/15.0 Uptime: 00:00:11 timeout: 248 Last reporter: 10.2.10.16
    Include source: 1.2.1.1, 1.3.1.1
VLAN: v44 Tag: 44 (Index: 5)
  Group: 225.0.0.1
  Receiver count: 1, Flags: <V2-hosts>
    ge-0/0/21.0 Uptime: 00:00:02 timeout: 257
VLAN: v110 Tag: 110 (Index: 4)
  Router interfaces:
    ge-0/0/3.0 static Uptime: 00:08:45
    ge-0/0/2.0 static Uptime: 00:08:45
    ge-0/0/4.0 dynamic Uptime: 00:16:41 timeout: 254
  Group: 225.0.0.3
  Receiver count: 1, Flags: <V2-hosts>
    ge-0/0/5.0 Uptime: 00:00:19 timeout: 259
  Group: 225.1.1.1
  Receiver count: 1, Flags: <V2-hosts>
    ge-0/0/5.0 Uptime: 00:22:43 timeout: 96
  Group: 225.2.2.2
  Receiver count: 1, Flags: <V2-hosts Static>
    ge-0/0/5.0 Uptime: 00:23:13
```

show igmp-snooping route

Syntax	show igmp-snooping route <brief detail> <ethernet-switching <brief detail vlan (vlan-id vlan-name)>> <inet <brief detail vlan (vlan-id vlan-name)>> <vlan vlan-id vlan-name>
Release Information	Command introduced in JUNOS Release 9.1 for EX Series switches.
Description	Display IGMP snooping route information.
Options	none—Display general parameters. brief detail—(Optional) Display the specified level of output. ethernet-switching—(Optional) Display Ethernet switching information. inet—(Optional) Display inet information. vlan vlan-id vlan-name —(Optional) Display route information for the specified VLAN.
Required Privilege Level	view
Related Topics	<ul style="list-style-type: none"> ■ show igmp-snooping statistics ■ show igmp-snooping vlans
List of Sample Output	show igmp-snooping route on page 61 show igmp-snooping route vlan v1 on page 62
Output Fields	Table 6 on page 61 lists the output fields for the show igmp-snooping route command. Output fields are listed in the approximate order in which they appear.

Table 6: show igmp-snooping route Output Fields

Field Name	Field Description
Table	(For internal use only. Value is always 0.)
VLAN	Name of the VLAN.
Group	Multicast group address.
Next-hop	ID associated with the next-hop device.

```

user@switch> show igmp-snooping route
show igmp-snooping route
VLAN          Group          Next-hop
V11           224.1.1.1, *   533
Interfaces: ge-0/0/13.0, ge-0/0/1.0
VLAN          Group          Next-hop

```

```
v12                224.1.1.3, *          534
Interfaces: ge-0/0/13.0, ge-0/0/0.0
```

show igmp-snooping route vlan v1 user@switch> **show igmp-snooping route vlan v1**
route vlan v1 Table: 0

VLAN	Group	Next-hop
v1	224.1.1.1, *	1266
	Interfaces: ge-0/0/0.0	
v1	224.1.1.3, *	1266
	Interfaces: ge-0/0/0.0	
v1	224.1.1.5, *	1266
	Interfaces: ge-0/0/0.0	
v1	224.1.1.7, *	1266
	Interfaces: ge-0/0/0.0	
v1	224.1.1.9, *	1266
	Interfaces: ge-0/0/0.0	
v1	224.1.1.11, *	1266
	Interfaces: ge-0/0/0.0	

show igmp-snooping statistics

Syntax	show igmp-snooping statistics
Release Information	Command introduced in JUNOS Release 9.1 for EX Series switches.
Description	Display IGMP snooping statistics.
Required Privilege Level	view
Related Topics	<ul style="list-style-type: none"> ■ show igmp-snooping route ■ show igmp-snooping vlans
List of Sample Output	show igmp-snooping statistics on page 63
Output Fields	Table 7 on page 63 lists the output fields for the show igmp-snooping statistics command. Output fields are listed in the approximate order in which they appear.

Table 7: show igmp-snooping statistics Output Fields

Field Name	Field Description
Bad length	IGMP packet has illegal or bad length.
Bad checksum	IGMP or IP checksum is incorrect.
Invalid interface	Packet was received through an invalid interface.
Receive unknown	Unknown IGMP type.
Timed out	Number of timeouts for all multicast groups.
IGMP Type	Type of IGMP message (Query, Report, Leave, or Other).
Received	Number of IGMP packets received.
Transmitted	Number of IGMP packets transmitted.
Recv Errors	Number of general receive errors.

```

show igmp-snooping statistics user@switch> show igmp-snooping statistics
Bad length: 0 Bad checksum: 0 Invalid interface: 0
Not local: 0 Receive unknown: 0 Timed out: 58

IGMP Type      Received      Transmitted    Recv Errors
Queries:        74295         0              0
Reports:       18148423     0             16333523
Leaves:         0             0              0
Other:          0             0              0

```

show igmp-snooping vlans

Syntax	show igmp-snooping vlans <brief detail> <vlan <i>vlan-id</i> <i>vlan-name</i> >
Release Information	Command introduced in JUNOS Release 9.1 for EX Series switches.
Description	Display IGMP snooping VLAN information.
Options	none—Display general parameters. brief detail—(Optional) Display the specified level of output. vlan <i>vlan-id</i> vlan <i>vlan-number</i> —(Optional) Display VLAN information for the specified VLAN.
Required Privilege Level	view
Related Topics	<ul style="list-style-type: none"> ■ show igmp-snooping route ■ show igmp-snooping statistics
List of Sample Output	<p>show igmp-snooping vlans on page 65</p> <p>show igmp-snooping vlans vlan v10 on page 65</p> <p>show igmp-snooping vlans vlan v10 detail on page 65</p>
Output Fields	Table 8 on page 64 lists the output fields for the show igmp-snooping vlans command. Output fields are listed in the approximate order in which they appear.

Table 8: show igmp-snooping vlans Output Fields

Field Name	Field Description	Level of Output
VLAN	Name of the VLAN.	All levels
Interfaces	Number of interfaces in the VLAN.	All levels
Groups	Number of groups in the VLAN	All levels
MRouters	Number of multicast routers associated with the VLAN.	All levels
Receivers	Number of host receivers in the VLAN.	All levels
Tag	Numerical identifier of the VLAN.	Detail
vlan-interface	Internal VLAN interface identifier.	Detail
Membership timeout	Membership timeout value.	Detail

Table 8: show igmp-snooping vlans Output Fields (continued)

Field Name	Field Description	Level of Output
Querier timeout	Timeout value for interfaces dynamically marked as router interfaces (interfaces that receive queries). When the querier timeout is reached, the switch marks the interface as a host interface.	Detail
Interface	Name of the interface.	Detail
Reporters	Number of dynamic groups on an interface.	Detail

```

show igmp-snooping user@switch> show igmp-snooping vlans
vlans
VLAN      Interfaces Groups MRouters Receivers
default   0         0         0         0
v1        11        50        0         0
v10       1         0         0         0
v11       1         0         0         0
v180     3         0         1         0
v181     3         0         0         0
v182     3         0         0         0

show igmp-snooping user@switch> show igmp-snooping vlans vlan v10
vlans vlan v10
user@switch> show igmp-snooping vlans vlan v10
VLAN      Interfaces Groups MRouters Receivers
v10       1         0         0         0

show igmp-snooping user@switch> show igmp-snooping vlans vlan v10 detail
vlans vlan v10 detail
VLAN: v10, Tag: 10, vlan-interface: vlan.10
Membership timeout: 260, Querier timeout: 255
Interface: ge-0/0/10.0, tagged, Groups: 0, Reporters: 0

```

