




Junos[®] OS for EX Series Ethernet Switches, Release 11.3: Multicast



Published: 2011-11-23
Revision 2

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

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

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

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

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

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

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

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

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

Junos® OS for EX Series Ethernet Switches, Release 11.3: Multicast

Copyright © 2011, Juniper Networks, Inc.

All rights reserved.

Revision History

November 2011—Revision 2

September 2011—Revision 1

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About This Topic Collection	vii
	How to Use This Guide	vii
	List of EX Series Guides for Junos OS Release 11.3	vii
	Downloading Software	ix
	Documentation Symbols Key	x
	Documentation Feedback	xi
	Requesting Technical Support	xii
	Self-Help Online Tools and Resources	xii
	Opening a Case with JTAC	xii
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	5
	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
	Understanding IGMP Snooping and Multicast Forwarding	10
	IGMP Snooping and Forwarding Interfaces	10
	General Forwarding Rules	11
	Examples of IGMP Snooping Multicast Forwarding	11
	Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts	11
	Scenario 2: Switch Forwarding Multicast Traffic to Another Switch	12
	Scenario 3: Switch Connected to Hosts Only (No IGMP Querier)	13
	Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs	14
Chapter 2	Examples: IGMP Snooping and Multicast Configuration	17
	Example: Configuring IGMP Snooping on EX Series Switches	17
	Example: Configuring Multicast VLAN Registration on EX Series Switches	20
Chapter 3	Configuring IGMP Snooping and Multicast	25
	Configuring IGMP Snooping (CLI Procedure)	25
	Configuring IGMP Snooping (J-Web Procedure)	26
	Changing the IGMP Snooping Group Query Membership Timeout Value (CLI Procedure)	29

	Configuring Multicast VLAN Registration (CLI Procedure)	30
Chapter 4	Verifying IGMP Snooping and Multicast	31
	Monitoring IGMP Snooping	31
	Verifying That the IGMP Snooping Group Query Timeout Value Has Been Changed Correctly	32
Chapter 5	Configuration Statements for IGMP Snooping and Multicast	35
	[edit protocols] Configuration Statement Hierarchy	35
	accounting (Per Interface)	42
	accounting (Protocol)	42
	address (Anycast RPs)	43
	address (Local RPs)	43
	anycast-pim	44
	assert-timeout	45
	auto-rp	46
	bootstrap	47
	bootstrap-export	48
	bootstrap-import	48
	bootstrap-priority	49
	data-forwarding	50
	dense-groups	51
	disable	51
	disable (PIM)	52
	disable	53
	dr-election-on-p2p	53
	dr-register-policy	54
	embedded-rp	54
	export (Bootstrap)	55
	family (Bootstrap)	56
	family (Local RP)	57
	graceful-restart	58
	group	58
	group	59
	group-limit	60
	group-ranges	61
	groups	62
	hello-interval	62
	hold-time	63
	igmp-snooping	64
	immediate-leave	65
	immediate-leave	66
	import (Bootstrap)	67
	import (PIM)	67
	infinity	68
	install	68
	interface	69
	interface	70
	interface	71
	join-load-balance	72

local	73
local-address	74
mapping-agent-election	75
maximum-rps	76
mode	77
multicast-router-interface	77
neighbor-policy	78
pim	79
priority (Bootstrap)	82
priority (PIM Interfaces)	83
priority (PIM RPs)	84
promiscuous-mode	84
proxy	85
query-interval	86
query-interval	87
query-last-member-interval	88
query-last-member-interval	89
query-response-interval	90
query-response-interval	91
receiver	91
restart-duration	92
rib-group	92
robust-count	93
robust-count	93
rp	94
rp-register-policy	95
rp-set	96
source	96
source	97
source-vlans	97
spt-threshold	98
ssm-map	98
static	99
static (IGMP Snooping)	100
static	101
traceoptions	102
traceoptions	105
traceoptions	107
version	109
version (PIM)	110
vlan	111
Chapter 6	Operational Commands for IGMP Snooping and Multicast 113
	clear igmp membership 114
	clear igmp statistics 118
	clear igmp-snooping membership 120
	clear igmp-snooping statistics 121
	clear multicast bandwidth-admission 122
	clear multicast scope 124

clear multicast sessions	125
clear multicast statistics	126
clear pim join	127
clear pim register	128
clear pim statistics	129
mtrace	131
mtrace from-source	133
mtrace monitor	136
mtrace to-gateway	138
show igmp group	141
show igmp interface	145
show igmp statistics	148
show igmp-snooping membership	151
show igmp-snooping route	153
show igmp-snooping statistics	155
show igmp-snooping vlans	157
show multicast flow-map	159
show multicast interface	161
show multicast mrimfo	163
show multicast next-hops	165
show multicast pim-to-igmp-proxy	167
show multicast pim-to-mld-proxy	169
show multicast route	171
show multicast rpf	176
show multicast scope	180
show multicast sessions	182
show multicast usage	185
show pim bootstrap	188
show pim interfaces	190
show pim join	193
show pim neighbors	199
show pim rps	203
show pim source	208
show pim statistics	210

About This Topic Collection

- [How to Use This Guide on page vii](#)
- [List of EX Series Guides for Junos OS Release 11.3 on page vii](#)
- [Downloading Software on page ix](#)
- [Documentation Symbols Key on page x](#)
- [Documentation Feedback on page xi](#)
- [Requesting Technical Support on page xii](#)

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.

Software features for EX Series switches are listed by platform and by Junos OS release in a standalone document. See [EX Series Switch Software Features Overview](#).

The release notes are at http://www.juniper.net/techpubs/en_US/junos11.3/information-products/topic-collections/release-notes/11.3/junos-release-notes-11.3.pdf.

List of EX Series Guides for Junos OS Release 11.3

Title	Description
<i>Complete Hardware Guide for EX2200 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX2200 Ethernet switches
<i>Complete Hardware Guide for EX3200 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX3200 Ethernet switches
<i>Complete Hardware Guide for EX3300 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX3300 Ethernet switches

Title	Description
<i>Complete Hardware Guide for EX4200 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX4200 Ethernet switches
<i>Complete Hardware Guide for EX4500 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX4500 Ethernet switches
<i>Complete Hardware Guide for EX6210 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX6210 Ethernet switches
<i>Complete Hardware Guide for EX8208 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8208 Ethernet switches
<i>Complete Hardware Guide for EX8216 Ethernet Switches</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for EX8216 Ethernet switches
<i>Complete Hardware Guide for the XRE200 External Routing Engine</i>	Component descriptions, site preparation, installation, replacement, and safety and compliance information for the XRE200 External Routing Engine
<i>Complete Software Guide for Junos® OS for EX Series Ethernet Switches, Release 11.3</i>	Software feature descriptions, configuration examples, and tasks for Junos OS for EX Series switches
Software Topic Collections	Software feature descriptions, configuration examples and tasks, and reference pages for configuration statements and operational commands (This information also appears in the <i>Complete Software Guide for Junos® OS for EX Series Ethernet Switches, Release 11.3.</i>)
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Access Control</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Configuration Management</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Class of Service</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Device Security</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Ethernet Switching</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: EX3300, EX4200, and EX4500 Virtual Chassis</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: EX8200 Virtual Chassis</i>	





Title	Description
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Fibre Channel over Ethernet</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: High Availability</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Interfaces</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Layer 3 Protocols</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: MPLS</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Multicast</i>	
<i>Junos® OS for EX Series Switches, Release 11.3: Network Management and Monitoring</i>	
<i>Junos® OS for EX Series Switches, Release 11.3: Port Security</i>	
<i>Junos® OS for EX Series Switches, Release 11.3: Power over Ethernet</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Routing Policy and Packet Filtering</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Software Installation</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: Spanning-Tree Protocols</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: System Monitoring</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: System Services</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: System Setup</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: User and Access Management</i>	
<i>Junos® OS for EX Series Ethernet Switches, Release 11.3: User Interfaces</i>	

Downloading Software

You can download Junos OS for EX Series switches from the Download Software area at <http://www.juniper.net/customers/support/> . To download the software, you must

have a Juniper Networks user account. For information about obtaining an account, see <http://www.juniper.net/entitlement/setupAccountInfo.do>.

Documentation Symbols Key

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

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

Documentation Feedback

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

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

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

IGMP Snooping and Multicast

- [Understanding IGMP Snooping and Multicast on page 3](#)
- [Examples: IGMP Snooping and Multicast Configuration on page 17](#)
- [Configuring IGMP Snooping and Multicast on page 25](#)
- [Verifying IGMP Snooping and Multicast on page 31](#)
- [Configuration Statements for IGMP Snooping and Multicast on page 35](#)
- [Operational Commands for IGMP Snooping and Multicast on page 113](#)

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](#)
- [Understanding IGMP Snooping and Multicast Forwarding on page 10](#)

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.

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 5](#)
- [How Hosts Join and Leave Multicast Groups on page 7](#)
- [IGMP Snooping Support for IGMPv3 on page 7](#)

How IGMP Snooping Works

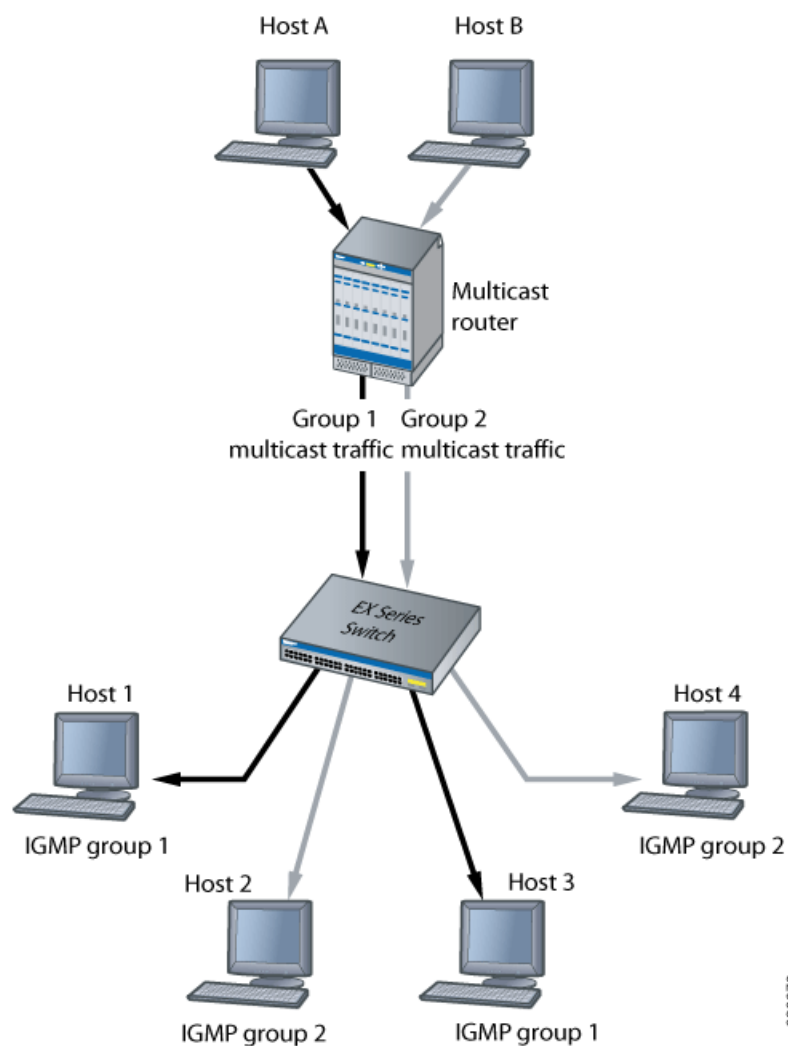
An EX Series switch usually learns *unicast* media access control (MAC) addresses by checking the source address field of the frames it receives. However, a *multicast* MAC

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. 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 a 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.

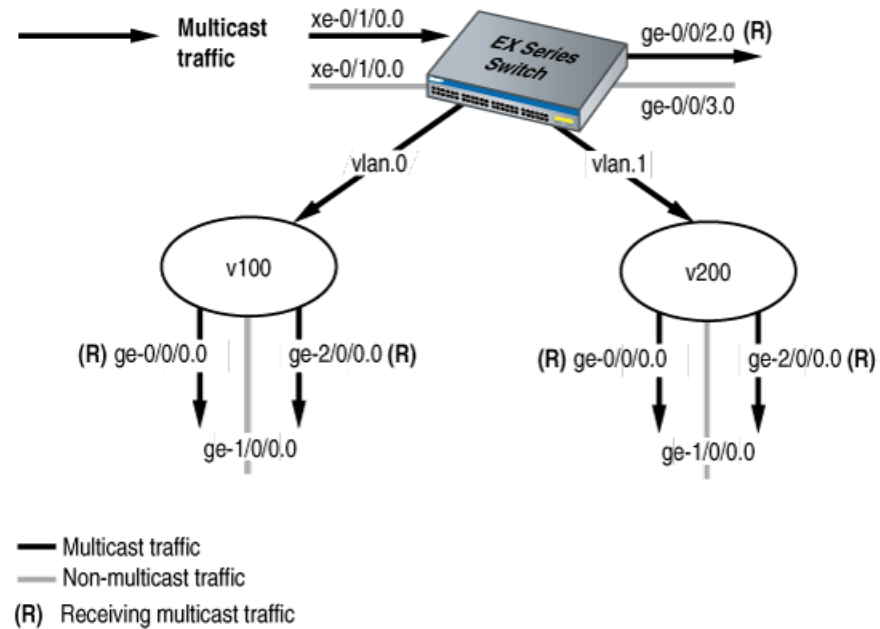
A bridge multicast ID is assigned to direct Layer 3 interfaces and to RVIs. For VLANs that include multicast receivers, the bridge multicast ID includes a sub-next-hop ID. The sub-next-hop ID identifies the multicast Layer 2 interfaces in that VLAN that are interested in receiving the multicast stream. 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



g020154

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.



NOTE: A host does not leave a group if its link goes down—for example, if a user disconnects from the port. The host remains a member of the group until group membership times out and a silent leave occurs. This means that if another user connects to the port before the silent leave occurs, the host resumes receiving the group multicast traffic until the silent leave, even though it never sent an IGMP join message.

IGMP Snooping Support for IGMPv3

IGMPv3 allows IGMP snooping to filter multicast streams based on the source address of the multicast stream. Junos operating system (Junos OS) for EX Series switches supports IGMPv3 packets that are in INCLUDE or EXCLUDE mode.

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).

When a host sends an IGMPv3 EXCLUDE report, the host indicates that it wants to join a multicast group and receive packets for that group *except* from those IP source addresses in the source-list parameter. However, because EX Series switches do not support forwarding on a per-source basis, the switch ignores the source information and creates a (*G,V) route. A host can also send an EXCLUDE report in which the source-list

parameter is empty, which is known as an EXCLUDE NULL report. An EXCLUDE NULL report indicates that the host wants to join the multicast group and receive packets from all sources. The switch creates a (*, G,V) route in this case also.

**Related
Documentation**

- [Understanding Multicast VLAN Registration on EX Series Switches on page 8](#)
- [Example: Configuring IGMP Snooping on EX Series Switches on page 17](#)
- [Configuring IGMP Snooping \(CLI Procedure\) on page 25](#)
- 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 Documentation

- [Example: Configuring Multicast VLAN Registration on EX Series Switches on page 20](#)
- [Configuring Multicast VLAN Registration \(CLI Procedure\) on page 30](#)

Understanding IGMP Snooping and Multicast Forwarding

IGMP snooping monitors the Internet Group Management Protocol (IGMP) traffic between hosts and multicast routers. The switch uses what IGMP snooping learns to forward multicast traffic only to interfaces that are connected to interested receivers. This conserves bandwidth by allowing the switch to send multicast traffic to only those interfaces that are connected to hosts that want to receive the traffic, instead of flooding the traffic to all interfaces in the VLAN. This topic describes how Juniper Networks EX Series Ethernet Switches forward multicast traffic when IGMP snooping is enabled.

This topic covers:

- [IGMP Snooping and Forwarding Interfaces on page 10](#)
- [General Forwarding Rules on page 11](#)
- [Examples of IGMP Snooping Multicast Forwarding on page 11](#)

IGMP Snooping and Forwarding Interfaces

To determine how to forward multicast traffic, IGMP snooping maintains information about the following interfaces in its multicast cache table:

- Multicast-router interfaces—These interfaces lead toward multicast routers or IGMP queriers.
- Group-member interfaces—These interfaces lead toward hosts that are members of multicast groups.

IGMP snooping learns about these interfaces by monitoring IGMP traffic. If an interface receives IGMP queries or Protocol Independent Multicast (PIM) updates, IGMP snooping adds the interface to its multicast cache table as a multicast-router interface. If an interface receives IGMP group membership reports in response to IGMP group queries or receives unsolicited join group messages, IGMP snooping adds the interface to its multicast cache table as a group-member interface.

Interfaces that IGMP snooping learns about are subject to aging. For example, if a multicast-router interface does not receive IGMP queries or PIM hellos within a certain interval, IGMP snooping removes that interface from its multicast cache table.



NOTE: For a switch to learn multicast-router interfaces and group-member interfaces, an IGMP querier must exist in the network. For the switch itself to function as an IGMP querier, IGMP must be enabled on the switch.

You can statically configure an interface to be a multicast-router interface or a group-member interface. A statically configured interface is not subject to aging and does not require an IGMP querier for IGMP snooping to learn about the interface. You can have a mix of statically configured and dynamically learned interfaces on a switch.

General Forwarding Rules

Multicast traffic received on a switch interface in a VLAN on which IGMP snooping is enabled is forwarded according to the following rules.

IGMP traffic is forwarded as follows:

- IGMP general queries received on a multicast-router interface are forwarded to all other interfaces in the VLAN.
- IGMP group-specific queries received on a multicast-router interface are forwarded to only those interfaces in the VLAN that are members of the group.
- IGMP reports received on a host interface are forwarded to multicast-router interfaces in the same VLAN, but not to the other host interfaces in the VLAN.

Multicast traffic that is not IGMP traffic is forwarded as follows:

- A multicast packet with a destination address of 224.0.0.0/24 is flooded to all other interfaces on the VLAN.
- An unregistered multicast packet—that is, a packet for a group that has no current members—is forwarded to all multicast-router interfaces in the VLAN.
- A registered multicast packet is forwarded only to those host interfaces in the VLAN that are members of the multicast group and to all multicast-router interfaces in the VLAN.

Examples of IGMP Snooping Multicast Forwarding

The following examples are provided to illustrate how IGMP snooping forwards multicast traffic in different topologies:

- [Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts on page 11](#)
- [Scenario 2: Switch Forwarding Multicast Traffic to Another Switch on page 12](#)
- [Scenario 3: Switch Connected to Hosts Only \(No IGMP Querier\) on page 13](#)
- [Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs on page 14](#)

Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts

In the topology shown in [Figure 3 on page 12](#), a switch acting as a pure Layer 2 device receives multicast traffic belonging to multicast group **239.10.1.1** from Source A, which is connected to the multicast router. It also receives multicast traffic belonging to multicast group **225.100.100.1** from Source B, which is connected directly to the switch. All interfaces on the switch belong to the same VLAN.

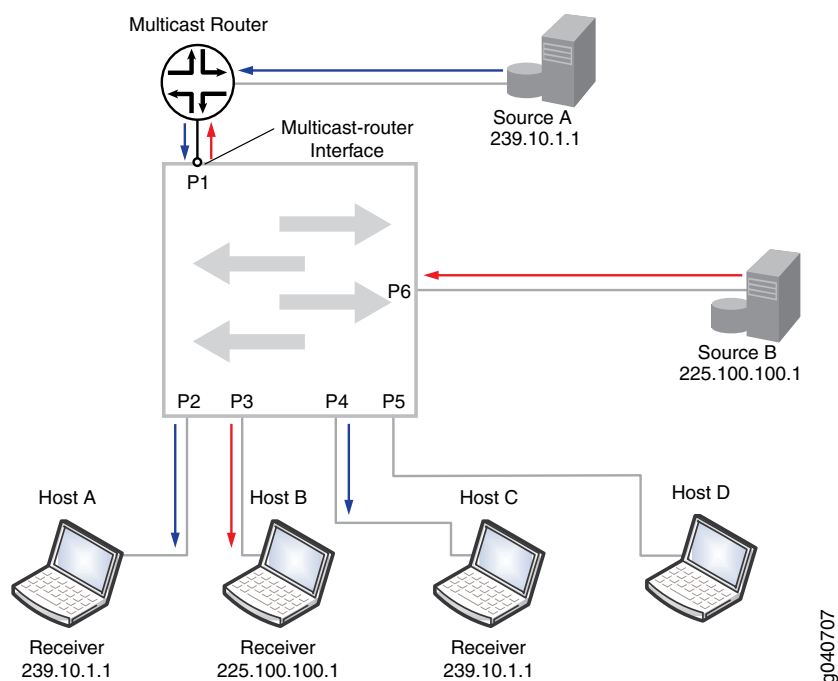
Because the switch receives IGMP queries from the multicast router on interface P1, IGMP snooping learns that interface P1 is a multicast-router interface and adds the interface to its multicast cache table. It forwards any IGMP general queries it receives on this

interface to all host interfaces on the switch, and, in turn, forwards membership reports it receives from hosts to the multicast-router interface.

In the example, Hosts A and C have responded to the membership queries with membership reports for group **239.10.1.1**. IGMP snooping adds interfaces P2 and P4 to its multicast cache table as member interfaces for group **239.10.1.1**. It forwards the group multicast traffic received from Source A to Hosts A and C, but not to Hosts B and D.

Host B has responded to the membership queries with a membership report for group **225.100.100.1**. The switch adds interface P3 to its multicast cache table as a member interface for group **225.100.100.1** and forwards multicast traffic it receives from Source B to Host B. The switch also forwards the multicast traffic it receives from Source B to the multicast-router interface P1.

Figure 3: Scenario 1: Switch Forwarding Multicast Router to a Multicast Router and Hosts



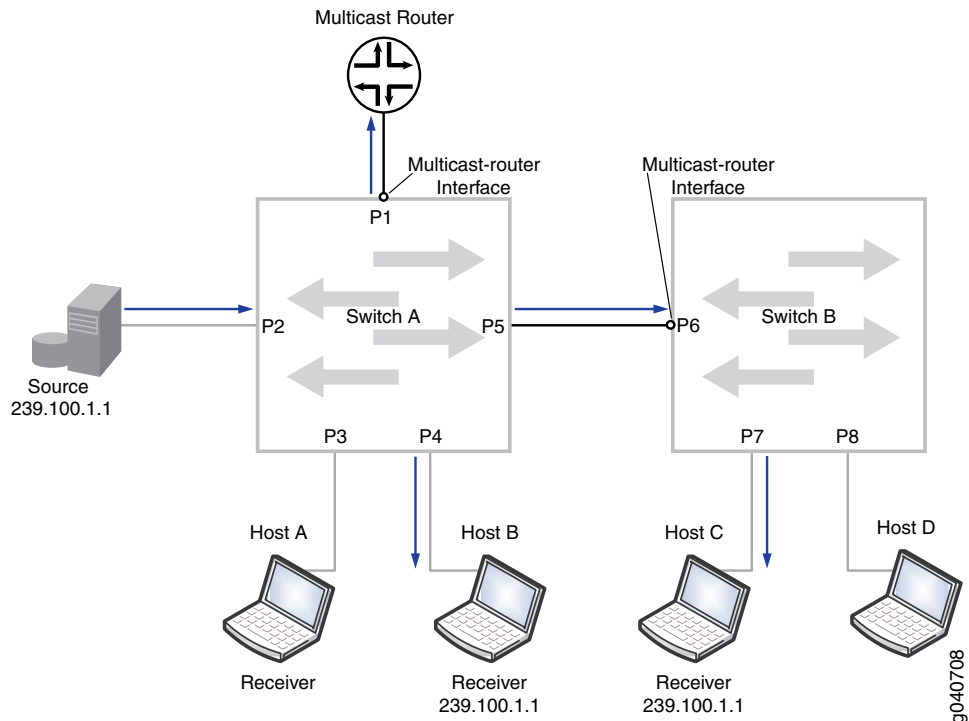
Scenario 2: Switch Forwarding Multicast Traffic to Another Switch

In the topology shown in [Figure 4 on page 13](#), a multicast source is connected to Switch A. Switch A in turn is connected to another switch, Switch B. Hosts on both Switch A and B are potential members of the multicast group. Both switches are acting as Layer 2 devices and all interfaces on the switches are members of the same VLAN.

Switch A receives IGMP queries from the multicast router on interface P1, making interface P1 a multicast-router interface for Switch A. Switch A forwards all general IGMP queries it receives on this interface to the other interfaces on the switch, including the interface connecting Switch B. Because Switch B receives the forwarded IGMP queries on interface P6, P6 is the multicast-router interface for Switch B. Switch B forwards the group

membership report it receives from Host C to Switch A through its multicast-router interface. Switch A forwards the membership report to its multicast-router interface, includes interface P5 in its multicast cache table as a group-member interface, and forwards multicast traffic from the source to Switch B.

Figure 4: Scenario 2: Switch Forwarding Multicast Traffic to Another Switch



You might have to configure P6 on Switch B as a static multicast-router interface in certain implementations. If Switch B receives unsolicited join messages from its hosts before it learns which interface is its multicast-router interface, it does not forward those reports to Switch A. When Switch A receives multicast traffic, it does not forward the traffic to Switch B, because it has not received any member reports on interface P5. You can statically configure interface P6 as a multicast-router interface to solve this issue.

Scenario 3: Switch Connected to Hosts Only (No IGMP Querier)

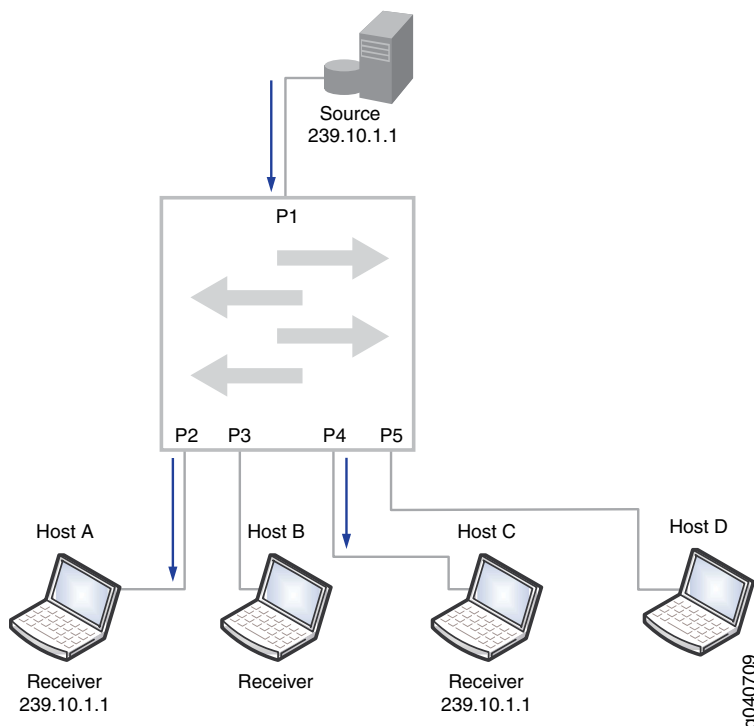
In the topology shown in [Figure 5 on page 14](#), a switch is connected to a multicast source and to hosts. There is no multicast router in this topology—hence there is no IGMP querier. Without an IGMP querier to respond to, a host does not send periodic membership reports. As a result, even if the host sends an unsolicited join to join a multicast group, its membership in the multicast group times out.

For IGMP snooping to work correctly in this network so that the switch forwards multicast traffic to Hosts A and C only, you can either:

- Configure interfaces P2 and P4 as static group-member interfaces.

- Configure a routed VLAN interface (RVI) on the VLAN and enable IGMP on it. In this case, the switch itself acts as an IGMP querier, and the hosts can dynamically join the multicast group and refresh their group membership by responding to the queries.

Figure 5: Scenario 3: Switch Connected to Hosts Only (No IGMP Querier)

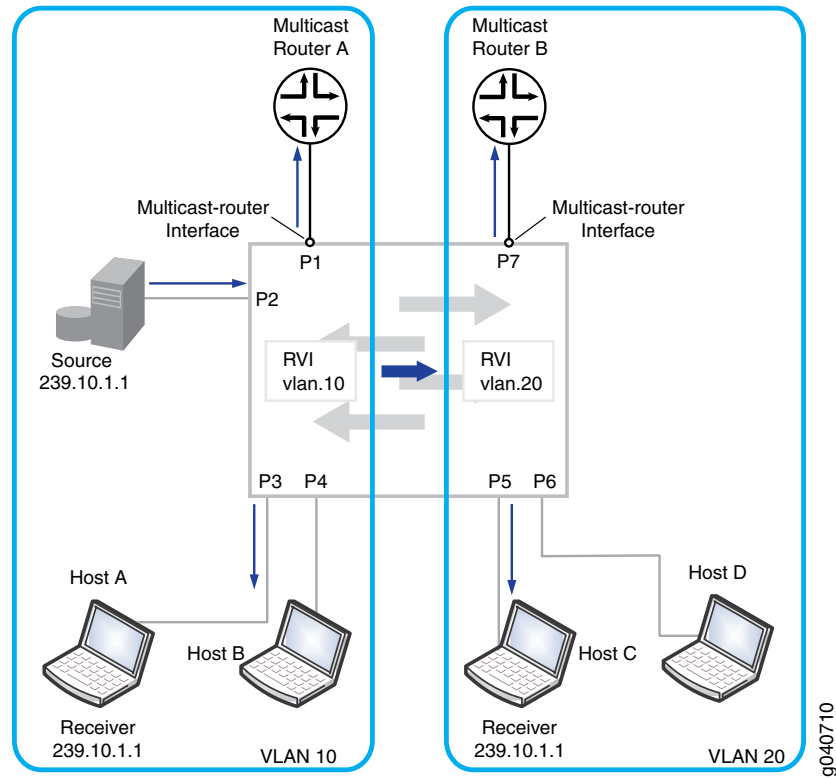


Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs

In the topology shown in [Figure 6 on page 15](#), a multicast source, Multicast Router A, and Hosts A and B are connected to the switch and are in VLAN 10. Multicast Router B and Hosts C and D are also connected to the switch and are in VLAN 20.

In a pure Layer 2 environment, traffic is not forwarded between VLANs. For Host C to receive the multicast traffic from the source on VLAN 10, RVIs must be created on VLAN 10 and VLAN 20 to permit routing of the multicast traffic between the VLANs. In addition, PIM must be enabled on the switch to perform the multicast routing.

Figure 6: Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs



Related Documentation

- [IGMP Snooping on EX Series Switches Overview on page 3](#)
- [Example: Configuring IGMP Snooping on EX Series Switches on page 17](#)
- [Configuring IGMP Snooping \(CLI Procedure\) on page 25](#)
- [Configuring IGMP Snooping \(J-Web Procedure\) on page 26](#)
- [Configuring Routed VLAN Interfaces \(CLI Procedure\)](#)

CHAPTER 2

Examples: IGMP Snooping and Multicast Configuration

- [Example: Configuring IGMP Snooping on EX Series Switches on page 17](#)
- [Example: Configuring Multicast VLAN Registration on EX Series Switches on page 20](#)

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 17](#)
- [Overview and Topology on page 18](#)
- [Configuration on page 18](#)

Requirements

This example uses the following software and hardware components:

- One EX3200-24T switch
- Junos OS 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 18](#) 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	employee-vlan , tag 20
Interfaces in employee-vlan	ge-0/0/1 , ge-0/0/2 , ge-0/0/3
Multicast IP address for employee-vlan	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 without waiting for any other IGMP messages to be exchanged (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 Documentation**
- [Configuring IGMP Snooping \(CLI Procedure\) on page 25](#)
 - [\[edit protocols\] Configuration Statement Hierarchy on page 35](#)

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 20](#)
- [Overview and Topology on page 20](#)
- [Configuration on page 23](#)

Requirements

This example uses the following hardware and software components:

- One EX Series switch
- Junos OS 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 7 on page 22](#) 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 7: MVR Topology in Transparent Mode

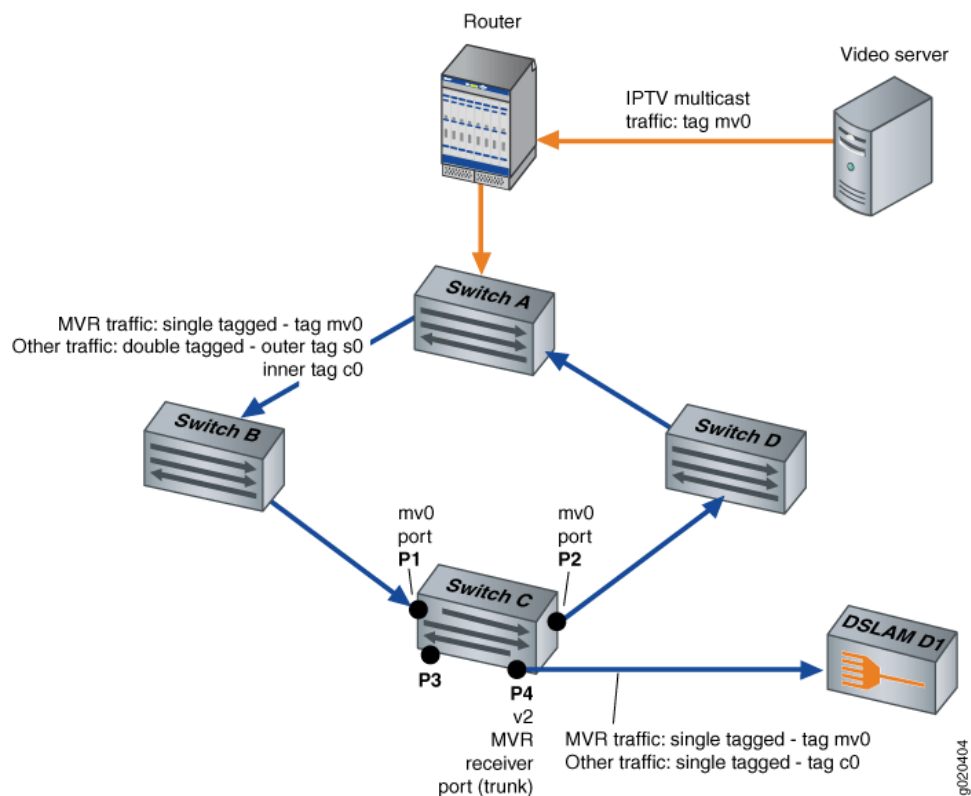
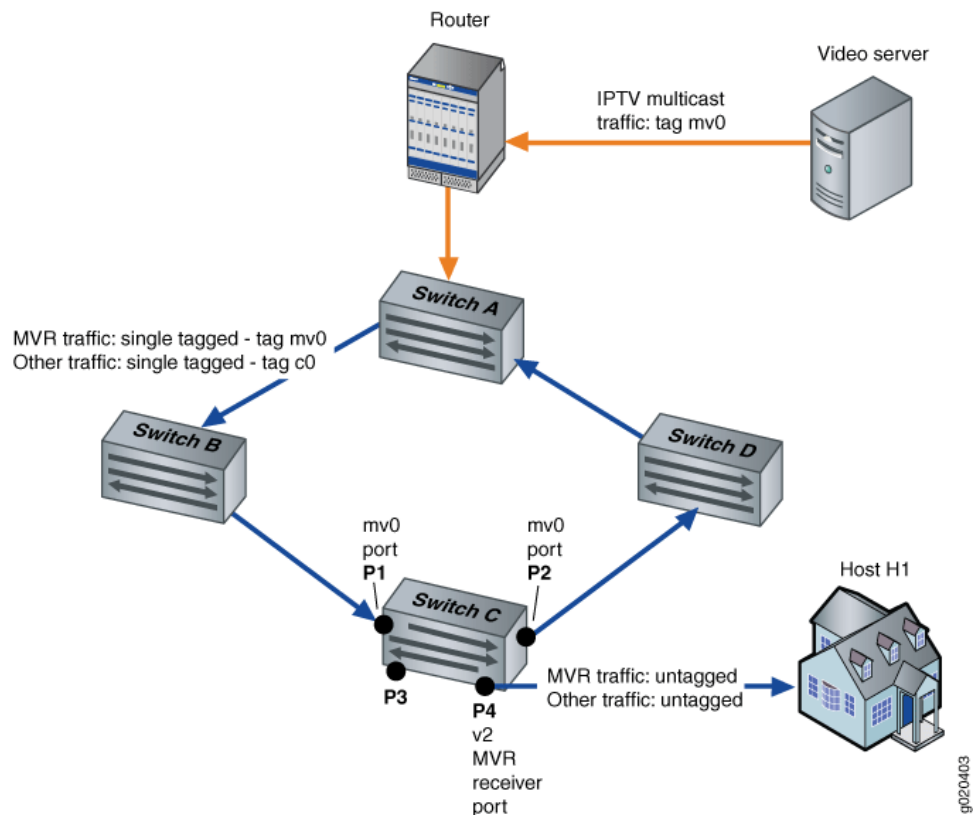


Figure 8 on page 23 shows the MVR topology in proxy mode. Interfaces P1 and P2 on switch C belong to MVLAN **mv0** and customer VLAN **c0**. Interface P4 on switch C is an access port of customer VLAN **c0**. In the upstream direction of the network, only non-IPTV traffic is being carried on customer 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 8: 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 Documentation**
- [Configuring Multicast VLAN Registration \(CLI Procedure\) on page 30](#)
 - [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 25](#)
- [Configuring IGMP Snooping \(J-Web Procedure\) on page 26](#)
- [Changing the IGMP Snooping Group Query Membership Timeout Value \(CLI Procedure\) on page 29](#)
- [Configuring Multicast VLAN Registration \(CLI Procedure\) on page 30](#)

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 group membership from an interface when it receives a leave message from that interface without waiting for any other IGMP messages to be exchanged (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 Documentation

- [Example: Configuring IGMP Snooping on EX Series Switches on page 17](#)
- [Changing the IGMP Snooping Group Query Membership Timeout Value \(CLI Procedure\) on page 29](#)
- [show igmp-snooping membership on page 151](#)
- [show igmp-snooping route on page 153](#)
- [show igmp-snooping statistics on page 155](#)
- [show igmp-snooping vlans on page 157](#)
- [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**.



NOTE: After you make changes to the configuration in this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options > Commit**. See [Using the Commit Options to Commit Configuration Changes](#) for details about all commit options.

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 27](#)

3. Click **OK** to apply changes to the configuration or click **Cancel** to 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 without waiting for any other IGMP messages to be exchanged (IGMPv2 only).	<p>To enable the option, select the check box.</p> <p>To disable the option, clear the check box.</p>
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 Documentation

- [Example: Configuring IGMP Snooping on EX Series Switches on page 17](#)
- [Configuring IGMP Snooping \(CLI Procedure\) on page 25](#)
- [Changing the IGMP Snooping Group Query Membership Timeout Value \(CLI Procedure\) on page 29](#)
- [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](#).

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 Documentation

- [Example: Configuring IGMP Snooping on EX Series Switches on page 17](#)
- [Verifying That the IGMP Snooping Group Query Timeout Value Has Been Changed Correctly on page 32](#)
- [Configuring IGMP Snooping \(CLI Procedure\) on page 25](#)
- [Configuring IGMP Snooping \(J-Web Procedure\) on page 26](#)

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 Documentation

- [Example: Configuring Multicast VLAN Registration on EX Series Switches on page 20](#)
- [Understanding Multicast VLAN Registration on EX Series Switches on page 8](#)

CHAPTER 4

Verifying IGMP Snooping and Multicast

- [Monitoring IGMP Snooping on page 31](#)
- [Verifying That the IGMP Snooping Group Query Timeout Value Has Been Changed Correctly on page 32](#)

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 31](#) 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	

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

Field	Values
VLAN	The VLAN for which IGMP snooping is enabled.
Group	Indicates the multicast groups learned by the VLAN.
Next-Hop	Specifies the next hop assigned by the switch after performing the route lookup.

- Related Documentation**
- [show igmp-snooping vlans on page 157](#)
 - [show igmp-snooping statistics on page 155](#)
 - [show igmp-snooping route on page 153](#)
 - [Configuring IGMP Snooping \(CLI Procedure\) on page 25](#)
 - [Example: Configuring IGMP Snooping on EX Series Switches on page 17](#)

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 Documentation**
- [Changing the IGMP Snooping Group Query Membership Timeout Value \(CLI Procedure\) on page 29](#)

CHAPTER 5

Configuration Statements for IGMP Snooping and Multicast

- [\[edit protocols\]](#) Configuration Statement Hierarchy on page 35

[\[edit protocols\]](#) 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 ) {
          eapol-block;
          block-interval block-interval;
        }
        server-timeout seconds;
        supplicant (multiple | single | single-secure);
        supplicant-timeout seconds;
        transmit-period seconds;
      }
    }
    no-mac-table-binding {
      authentication-profile-name
      interface
```

```

    }
    static mac-address {
        interface interface-name;
        vlan-assignment (vlan-id |vlan-name);
    }
}
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 (LLDP);
    advertisement-interval seconds;
    hold-multiplier number;
    interface (LLDP) (all | interface-name) {
        disable (LLDP);
    }
    lldp-configuration-notification-interval seconds;
    management-address ip-management-address;
    ptopo-configuration-maximum-hold-time seconds;
    ptopo-configuration-trap-interval seconds;
    traceoptions (LLDP) {
        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) {
    arp-on-stp
    bpdu-timeout-action {
      block;
      log;
    }
    cost cost;
    disable;
    disable;
    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 {
    connectivity-fault-management {
      action-profile profile-name {
        default-actions {
          interface-down;
        }
      }
    }
    linktrace {
      age (30m | 10m | 1m | 30s | 10s);
      path-database-size path-database-size;
    }
    maintenance-domain domain-name {
      level number;
      mip-half-function (none | default | explicit);
      name-format (character-string | none | dns | mac+2oct);
      maintenance-association ma-name {
        continuity-check {
          hold-interval minutes;
          interval (10m | 10s | 1m | 1s | 100ms);
          loss-threshold number;
        }
        mep mep-id {
          auto-discovery;
          direction down;
          interface interface-name;
          remote-mep mep-id {
            action-profile profile-name;
          }
        }
      }
    }
  }
}

```

```

    }
  }
  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;
    arp-on-stp
      bpdu-timeout-action {
        block;
        log;
      }
    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 {
    agent-id;
    collector {
      ip-address;
      udp-port port-number;
    }
    disable;
    interfaces interface-name {
      disable;
      polling-interval seconds;
      sample-rate {
        egress number;
        ingress number;
      }
    }
    polling-interval seconds;
    sample-rate {
      egress number;
      ingress number;
    }
    source-ip;
  }
  stp {
    disable;
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
      disable;
      arp-on-stp
        bpdv-timeout-action {
          block;
          log;
        }
      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;
  }
  uplink-failure-detection {
    group {
      group-name {
```

```

        link-to-monitor {
            interface-name;
        }
        link-to-disable {
            interface-name;
        }
    }
}
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) {
            arp-on-stp
                bpdu-timeout-action {
                    log;
                    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 Documentation

- 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 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 Multiple VLAN Registration Protocol (MVRP) on EX Series Switches
- Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch

- Understanding Ethernet OAM Link Fault Management for an EX Series Switch
- 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 Uplink Failure Detection

accounting (Per Interface)

Syntax	(accounting no-accounting);
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Enable or disable the collection of IGMP join and leave event statistics for an interface.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Recording IGMP Join and Leave Events

accounting (Protocol)

Syntax	accounting;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp], [edit protocols igmp]
Release Information	Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Enable the collection of IGMP join and leave event statistics on the system.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Recording IGMP Join and Leave Events

address (Anycast RPs)

Syntax	<code>address <i>address</i> <forward-msdp-sa>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols <code>pim rp local</code> (inet inet6) <code>anycast-pim rp-set</code>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols <code>pim rp local</code> (inet inet6) <code>anycast-pim rp-set</code>], [edit protocols <code>pim rp local</code> (inet inet6) <code>anycast-pim rp-set</code>], [edit routing-instances <i>routing-instance-name</i> protocols <code>pim rp local</code> (inet inet6) <code>anycast-pim rp-set</code>]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the anycast rendezvous point (RP) addresses in the RP set. Multiple addresses can be configured in an RP set. If the RP has peer Multicast Source Discovery Protocol (MSDP) connections, then the RP must forward MSDP source active (SA) messages.
Options	<i>address</i> —RP address in an RP set. <i>forward-msdp-sa</i> —(Optional) Forward MSDP SAs to this address.
Required Privilege Level	routing —To view this statement in the configuration. routing-control —To add this statement to the configuration.

address (Local RPs)

Syntax	<code>address <i>address</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols <code>pim rp local family</code> (inet inet6)], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols <code>pim rp local family</code> (inet inet6)], [edit protocols <code>pim rp local family</code> (inet inet6)], [edit routing-instances <i>routing-instance-name</i> protocols <code>pim rp local family</code> (inet inet6)]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the local rendezvous point (RP) address.
Options	<i>address</i> —Local RP address.
Required Privilege Level	routing —To view this statement in the configuration. routing-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring Local PIM RPs

anycast-pim

Syntax	<pre>anycast-pim { rp-set { address address <forward-msdp-sa>; } }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp local family (inet inet6)], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp local family (inet inet6)], [edit protocols pim rp local family (inet inet6)], [edit routing-instances <i>routing-instance-name</i> protocols pim rp local family (inet inet6)]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure properties for anycast RP using PIM. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring PIM Anycast With or Without MSDP

assert-timeout

Syntax	<code>assert-timeout <i>seconds</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim],</p> <p>[edit protocols pim],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	<p>Multicast routing devices running PIM sparse mode often forward the same stream of multicast packets onto the same LAN through the rendezvous-point tree (RPT) and shortest-path tree (SPT). PIM assert messages help routing devices determine which routing device forwards the traffic and prunes the RPT for this group. By default, routing devices enter an assert cycle every 180 seconds. You can configure this assert timeout to be between 5 and 210 seconds.</p>
Options	<p><i>seconds</i>—Time for routing device to wait before another assert message cycle.</p> <p>Range: 5 through 210 seconds</p> <p>Default: 180 seconds</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 Documentation	<ul style="list-style-type: none"> Example: Configuring the PIM Assert Timeout

auto-rp

Syntax	<pre>auto-rp { (announce discovery mapping); (mapping-agent-election no-mapping-agent-election); }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp], [edit protocols pim rp], [edit routing-instances <i>routing-instance-name</i> protocols pim rp]
Release Information	Statement introduced in Junos OS Release 7.5. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure automatic RP announcement and discovery.
Options	<p>announce—Configures the routing device to listen only for mapping packets and also to advertise itself if it is an RP.</p> <p>discovery—Configures the routing device to listen only for mapping packets.</p> <p>mapping—Configures the routing device to announce, listens for and generates mapping packets, and announces that the routing device is eligible to be an RP.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring PIM Auto-RP

bootstrap

Syntax	<pre>bootstrap { family (inet inet6) { export [<i>policy-names</i>]; import [<i>policy-names</i>]; priority <i>number</i>; } }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp],</p> <p>[edit protocols pim rp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp]</p>
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	<p>Configure parameters to control bootstrap routers and messages.</p> <p>The remaining statements are explained separately.</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 Documentation	<ul style="list-style-type: none"> Configuring PIM Bootstrap Properties for IPv4 Configuring PIM Bootstrap Properties for IPv4 or IPv6

bootstrap-export

Syntax	<code>bootstrap-export [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp], [edit protocols pim rp], [edit routing-instances <i>routing-instance-name</i> protocols pim rp]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Apply one or more export policies to control outgoing PIM bootstrap messages.
Options	<i>policy-names</i> —Name of one or more import policies.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring PIM Bootstrap Properties for IPv4Configuring PIM Bootstrap Properties for IPv4 or IPv6bootstrap-import on page 48

bootstrap-import

Syntax	<code>bootstrap-import [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp], [edit protocols pim rp], [edit routing-instances <i>routing-instance-name</i> protocols pim rp]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Apply one or more import policies to control incoming PIM bootstrap messages.
Options	<i>policy-names</i> —Name of one or more import policies.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring PIM Bootstrap Properties for IPv4Configuring PIM Bootstrap Properties for IPv4 or IPv6bootstrap-export on page 48

bootstrap-priority

Syntax	<code>bootstrap-priority <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp], [edit protocols pim rp], [edit routing-instances <i>routing-instance-name</i> protocols pim rp]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure whether this routing device is eligible to be a bootstrap router. In the case of a tie, the routing device with the highest IP address is elected to be the bootstrap router.
Options	<i>number</i> —Priority for becoming the bootstrap router. A value of 0 means that the routing device is not eligible to be the bootstrap router. Range: 0 through 255 Default: 0
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring PIM Bootstrap Properties for IPv4

data-forwarding

Syntax	<pre>data-forwarding { source { groups <i>group-prefix</i>; } receiver { source-vlans <i>vlan-list</i>; install; } }</pre>
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-number</i>]
Release Information	Statement introduced in Junos OS Release 9.6 for EX Series switches.
Description	<p>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.</p> <p>The remaining statements are explained separately.</p>
Default	Disabled.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• [edit protocols] Configuration Statement Hierarchy on page 35• Example: Configuring Multicast VLAN Registration on EX Series Switches on page 20• Configuring Multicast VLAN Registration (CLI Procedure) on page 30

dense-groups

Syntax	<code>dense-groups { <i>addresses</i>; }</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure which groups are operating in dense mode.
Options	<i>addresses</i> —Address of groups operating in dense mode.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring PIM Sparse-Dense Mode Properties

disable

Syntax	<code>disable { interface <i>interface-name</i> }</code>
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-name</i>]
Release Information	Statement introduced in Junos OS 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 Documentation	<ul style="list-style-type: none"> Example: Configuring IGMP Snooping on EX Series Switches on page 17 Configuring IGMP Snooping (CLI Procedure) on page 25

disable (PIM)

Syntax	disable;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> protocols pim family (inet inet6)], [edit logical-systems <i>logical-system-name</i> protocols pim interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> protocols pim rp local family (inet inet6)], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp local family (inet inet6)], [edit protocols pim], [edit protocols pim family (inet inet6)], [edit protocols pim interface <i>interface-name</i>], [edit protocols pim rp local family (inet inet6)], [edit routing-instances <i>routing-instance-name</i> protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim family (inet inet6)], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols pim rp local family (inet inet6)]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>disable statement extended to the [family] hierarchy level in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Explicitly disable PIM at the protocol, interface or family hierarchy levels.
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 Documentation	<ul style="list-style-type: none">Disabling PIMfamily (Disable PIM)

disable

Syntax	disable;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Disable IGMP on the system.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Disabling IGMP

dr-election-on-p2p

Syntax	dr-election-on-p2p;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Enable PIM designated router (DR) election on point-to-point (P2P) links.
Default	No PIM DR election is performed on P2P links.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring PIM Designated Router Election on Point-to-Point Links

dr-register-policy

Syntax	<code>dr-register-policy [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp], [edit protocols pim rp], [edit routing-instances <i>routing-instance-name</i> protocols pim rp]
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Apply one or more policies to control outgoing PIM register messages.
Options	<i>policy-names</i> —Name of one or more import policies.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring Register Message Filters on a PIM RP and DRrp-register-policy on page 95

embedded-rp

Syntax	<pre>embedded-rp { group-ranges { <i>destination-ip-prefix</i> </<i>prefix-length</i>>; } maximum-rps <i>limit</i>; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp], [edit protocols pim rp], [edit routing-instances <i>routing-instance-name</i> protocols pim rp]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure properties for embedded IP version 6 (IPv6) RPs. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring PIM Embedded RP for IPv6

export (Bootstrap)

Syntax	<code>export [<i>policy-names</i>];</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp bootstrap family (inet inet6)],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap family (inet inet6)],</p> <p>[edit protocols pim rp bootstrap family (inet inet6)],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap family (inet inet6)]</p>
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Apply one or more export policies to control outgoing PIM bootstrap messages.
Options	<i>policy-names</i> —Name of one or more import policies.
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 Documentation	<ul style="list-style-type: none"> Configuring PIM Bootstrap Properties for IPv4 Configuring PIM Bootstrap Properties for IPv4 or IPv6 import (Bootstrap) on page 67

family (Bootstrap)

Syntax	<pre>family (inet inet6) { export [<i>policy-names</i>]; number; [<i>policy-names</i>]; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp bootstrap], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap], [edit protocols pim rp bootstrap], [edit routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap]
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure which IP protocol type bootstrap properties to apply.
Options	<p>inet—Apply IP version 4 (IPv4) local RP properties.</p> <p>inet6—Apply IPv6 local RP properties.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring PIM Bootstrap Properties for IPv4Configuring PIM Bootstrap Properties for IPv4 or IPv6

family (Local RP)

Syntax	<pre> family (inet inet6) { disable; address address; anycast-pim { local-address address; rp-set { address address <forward-msdp-sa>; } } group-ranges { destination-ip-prefix </prefix-length>; } hold-time seconds; priority number; } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp local],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp local],</p> <p>[edit protocols pim rp local],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp local]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Configure which IP protocol type local RP properties to apply.
Options	<p>inet—Apply IP version 4 (IPv4) local RP properties.</p> <p>inet6—Apply IPv6 local RP properties.</p> <p>The remaining statements are explained separately.</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 Documentation	<ul style="list-style-type: none"> Configuring Local PIM RPs

graceful-restart

Syntax	<code>graceful-restart { disable; restart-duration seconds; }</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure PIM sparse mode graceful restart. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring PIM Sparse Mode Graceful Restart

group

Syntax	<code>group <i>ip-address</i>;</code>
Hierarchy Level	[edit protocols igmp-snooping <i>vlan</i> <i>vlan-id</i> <i>vlan-name</i> interface <i>interface-name</i> static (IGMP Snooping)]
Release Information	Statement introduced in Junos OS 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 Documentation	<ul style="list-style-type: none">Example: Configuring IGMP Snooping on EX Series Switches on page 17Configuring IGMP Snooping (CLI Procedure) on page 25

group

Syntax `group multicast-group-address {
 exclude;
 group-count number;
 group-increment increment;
 source ip-address {
 source-count number;
 source-increment increment;
 }
}`

Hierarchy Level [edit logical-systems *logical-system-name* protocols igmp **interface** *interface-name* **static**],
 [edit protocols igmp **interface** *interface-name* **static**]

Release Information Statement introduced before Junos OS Release 7.4.
 Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the IGMP multicast group address and (optionally) the source address for the multicast group being statically configured on an interface.



NOTE: You must specify a unique address for each group.

The remaining statements are explained separately.

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

Related Documentation

- Enabling IGMP Static Group Membership

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 OS 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	limit —Number that represents the maximum number of multicast groups allowed on the specified interface. Range: 0 through 65535
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring IGMP Snooping on EX Series Switches on page 17• Configuring IGMP Snooping (CLI Procedure) on page 25• Configuring IGMP Snooping (J-Web Procedure) on page 26• group on page 58

group-ranges

Syntax	<pre>group-ranges { destination-ip-prefix</prefix-length>; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp embeddedd-rp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp embeddedd-rp],</p> <p>[edit protocols pim rp embeddedd-rp],</p> <p>[edit protocols pim rp local family (inet inet6)],</p> <p>[edit protocols pim rp static address <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp embeddedd-rp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp local family (inet inet6)],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp static address <i>address</i>]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Configure the address ranges of the multicast groups for which this routing device can be an RP.
Default	The routing device is eligible to be the RP for all IPv4 or IPv6 groups (224.0.0.0/4 or FF70::/12 to FFF0::/12).
Options	<i>destination-mask</i> —Addresses or address ranges for which this routing device can be an RP.
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 Documentation	<ul style="list-style-type: none"> Configuring Local PIM RPs Configuring PIM Embedded RP for IPv6

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 OS Release 9.6 for EX Series switches.
Description	Specify the IP address range of the multicast VLAN (MVLAN) source interfaces.
Default	Disabled.
Options	group-prefix —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 Documentation	<ul style="list-style-type: none">• [edit protocols] Configuration Statement Hierarchy on page 35• Example: Configuring Multicast VLAN Registration on EX Series Switches on page 20• Configuring Multicast VLAN Registration (CLI Procedure) on page 30

hello-interval

Syntax	<code>hello-interval seconds;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i>], [edit protocols pim interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify how often the router sends PIM hello packets out of an interface.
Options	seconds —Length of time between PIM hello packets. Range: 0 through 255 Default: 30 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• hold-time on page 63• Modifying the PIM Hello Interval

hold-time

Syntax	<code>hold-time <i>seconds</i>;</code>
Hierarchy Level	[edit protocols <code>pim rp local family</code> (inet inet6)], [edit routing-instances <i>routing-instance-name</i> protocols <code>pim rp local family</code> (inet inet6)]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the time period for which a neighbor is to consider the sending routing device (this routing device) to be operative (up).
Options	<i>seconds</i> —Hold time. Range: 0 through 255 Default: 150 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring Local PIM RPs

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 (IGMP Snooping) {
                    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 OS 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 Documentation

- [Example: Configuring IGMP Snooping on EX Series Switches on page 17](#)
- [Configuring IGMP Snooping \(CLI Procedure\) on page 25](#)

immediate-leave

Syntax	immediate-leave;
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-name</i>]
Release Information	Statement introduced in Junos OS 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 without waiting for any other IGMP messages to be exchanged.
	<div>  <p>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.</p> </div>
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 Documentation	<ul style="list-style-type: none"> • Example: Configuring IGMP Snooping on EX Series Switches on page 17 • Configuring IGMP Snooping (CLI Procedure) on page 25

immediate-leave

Syntax	immediate-leave;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>When this statement is enabled on a routing device running IGMP version 2 (IGMPv2), after the routing device receives a leave group membership message from a host associated with the interface, the routing device immediately removes the group membership from the interface and suppresses the sending of any group-specific queries for the multicast group.</p> <p>When this statement is enabled on a routing device running IGMP version 3 (IGMPv3), after the routing device receives a report with the type BLOCK_OLD_SOURCES, the routing device suppresses the sending of group-and-source queries but relies on the Junos OS-supported host tracking mechanism to determine whether or not it removes a particular source group membership from the interface.</p>
	<div><p>NOTE: When issuing this command on IGMPv2 interfaces, ensure that the IGMP interface has only one IGMP host connected. If more than one IGMPv2 host is connected to a LAN through the same interface, and one host sends a done message, the routing device removes all hosts on the interface from the multicast group. The routing device loses contact with the hosts that properly remain in the multicast group until they send join requests in response to the next general multicast listener query from the router.</p></div>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Specifying Immediate-Leave Host Removal for IGMP

import (Bootstrap)

Syntax	<code>import [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp bootstrap (inet inet6)], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap (inet inet6)], [edit protocols pim rp bootstrap (inet inet6)], [edit routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap (inet inet6)]
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Apply one or more import policies to control incoming PIM bootstrap messages.
Options	<i>policy-names</i> —Name of one or more import policies.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring PIM Bootstrap Properties for IPv4 Configuring PIM Bootstrap Properties for IPv4 or IPv6 export (Bootstrap) on page 55

import (PIM)

Syntax	<code>import [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Apply one or more policies to routes being imported into the routing table from PIM. Use the import statement to filter PIM join messages from entering the network.
Options	<i>policy-names</i> —Name of one or more policies.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Filtering Incoming PIM Join Messages

infinity

Syntax	<code>infinity [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim spt-threshold], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim spt-threshold], [edit protocols pim spt-threshold], [edit routing-instances <i>routing-instance-name</i> protocols pim spt-threshold]
Release Information	Statement introduced in Junos OS Release 8.0. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Apply one or more policies to set the SPT threshold to infinity for a source-group address pair. Use the infinity statement to prevent the last-hop routing device from transitioning from the RPT rooted at the RP to an SPT rooted at the source for that source-group address pair.
Options	<i>policy-names</i> —Name of one or more policies.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring the PIM SPT Threshold Policy

install

Syntax	<code>install;</code>
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-number</i> data-forwarding receiver]
Release Information	Statement introduced in Junos OS 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 Documentation	<ul style="list-style-type: none">• [edit protocols] Configuration Statement Hierarchy on page 35• Example: Configuring Multicast VLAN Registration on EX Series Switches on page 20• Configuring Multicast VLAN Registration (CLI Procedure) on page 30

interface

Syntax	<pre> interface (all <i>interface-name</i>) { accept-remote-source; disable; bfd-liveness-detection { authentication { algorithm <i>algorithm-name</i>; key-chain <i>key-chain-name</i>; loose-check; } detection-time { threshold <i>milliseconds</i>; } minimum-interval <i>milliseconds</i>; minimum-receive-interval <i>milliseconds</i>; multiplier <i>number</i>; version (0 1 automatic); } family (inet inet6) { disable; } hello-interval <i>seconds</i>; mode (dense sparse sparse-dense); neighbor-policy [<i>policy-names</i>]; override-interval <i>milliseconds</i>; priority <i>number</i>; propagation-delay <i>milliseconds</i>; reset-tracking-bit; version <i>version</i>; } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Enable PIM on an interface and configure interface-specific properties.
Options	<p><i>interface-name</i>—Name of the interface. Specify the full interface name, including the physical and logical address components. To configure all interfaces, you can specify all.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.</p>

Related Documentation

- [PIM on Aggregated Interfaces](#)

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 OS Release 9.1 for EX Series switches.

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

Default None.

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

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- [show igmp-snooping vlans on page 157](#)
- [Example: Configuring IGMP Snooping on EX Series Switches on page 17](#)
- [Configuring IGMP Snooping \(CLI Procedure\) on page 25](#)

interface

Syntax	<pre> interface <i>interface-name</i> { disable; (accounting no-accounting); group-limit <i>limit</i>; group-policy [<i>policy-names</i>]; immediate-leave; oif-map <i>map-name</i>; passive; promiscuous-mode; ssm-map <i>ssm-map-name</i>; static { group <i>multicast-group-address</i> { exclude; group-count <i>number</i>; group-increment <i>increment</i>; source <i>ip-address</i> { source-count <i>number</i>; source-increment <i>increment</i>; } } } version <i>version</i>; } </pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp], [edit protocols igmp]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Enable IGMP on an interface and configure interface-specific properties.
Options	<p><i>interface-name</i>—Name of the interface. Specify the full interface name, including the physical and logical address components. To configure all interfaces, you can specify all.</p> <p>The remaining statements are explained separately.</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 Documentation	<ul style="list-style-type: none"> Enabling IGMP

join-load-balance

Syntax	join-load-balance;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim]
Release Information	Statement introduced in Junos OS Release 9.0. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Enable load balancing of PIM join messages across interfaces and routing devices.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring PIM Join Load Balancingclear pim join-distribution in the Junos OS Routing Protocols and Policies Command Reference

local

Syntax	<pre> local { disable; address address; family (inet inet6) { disable; address address; anycast-pim { local-address address; rp-set { address address <forward-msdp-sa>; } } group-ranges { destination-ip-prefix</prefix-length>; } hold-time seconds; priority number; } group-ranges { destination-ip-prefix</prefix-length>; } hold-time seconds; priority number; } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp],</p> <p>[edit protocols pim rp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>The remaining statements are explained separately.</p>
Description	Configure the routing device's RP properties.
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 Documentation	<ul style="list-style-type: none"> Configuring Local PIM RPs

local-address

Syntax	<code>local-address <i>address</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp local family (inet inet6) anycast-pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp local family (inet inet6) anycast-pim], [edit protocols pim rp local family (inet inet6) anycast-pim], [edit routing-instances <i>routing-instance-name</i> protocols pim rp local family (inet inet6) anycast-pim]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the routing device's local address for anycast rendezvous point (RP). If this statement is omitted, the router ID is used as this address.
Options	<i>address</i> —Anycast RP IPv4 or IPv6 address, depending on family configuration.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Example: Configuring PIM Anycast With or Without MSDP

mapping-agent-election

Syntax	(mapping-agent-election no-mapping-agent-election);
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp auto-rp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp auto-rp], [edit protocols pim rp auto-rp], [edit routing-instances <i>routing-instance-name</i> protocols pim rp auto-rp]
Release Information	Statement introduced in Junos OS Release 7.5. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the routing device's mapping announcements as a mapping agent.
Options	<p>mapping-agent-election—Mapping agents do not announce mappings when receiving mapping messages from a higher-addressed mapping agent.</p> <p>no-mapping-agent-election—Mapping agents always announce mappings and do not perform mapping agent election.</p> <p>Default: mapping-agent-election</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 Documentation	<ul style="list-style-type: none"> Configuring PIM Auto-RP

maximum-rps

Syntax	<code>maximum-rps <i>limit</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp embedded-rp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp embedded-rp], [edit protocols pim rp embedded-rp], [edit routing-instances <i>routing-instance-name</i> protocols pim rp embedded-rp]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Limit the number of RPs that the routing device acknowledges.
Options	<i>limit</i> —Number of RPs. Range: 1 through 500 Default: 100
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring PIM Embedded RP for IPv6

mode

Syntax	mode (dense sparse sparse-dense);
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim interface interface-name], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim interface interface-name], [edit protocols pim interface interface-name], [edit routing-instances <i>routing-instance-name</i> protocols pim interface interface-name]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure PIM to operate in sparse, dense, or sparse-dense mode.
Options	dense —Operate in dense mode. sparse —Operate in sparse mode. sparse-dense —Operate in sparse-dense mode. Default: sparse
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring PIM Dense Mode Properties Configuring PIM Sparse-Dense Mode Properties

multicast-router-interface

Syntax	multicast-router-interface;
Hierarchy Level	[edit protocols igmp-snooping vlan vlan-id <i>vlan-name</i> interface interface-name]
Release Information	Statement introduced in Junos OS 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 Documentation	<ul style="list-style-type: none"> Example: Configuring IGMP Snooping on EX Series Switches on page 17 Configuring IGMP Snooping (CLI Procedure) on page 25

neighbor-policy

Syntax	<code>neighbor-policy [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols <code>pim interface interface-name</code>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols <code>pim interface interface-name</code>], [edit protocols <code>pim interface interface-name</code>], [edit routing-instances <i>routing-instance-name</i> protocols <code>pim interface interface-name</code>]
Release Information	Statement introduced in Junos OS Release 8.2. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Apply a PIM interface-level policy to filter neighbor IP addresses.
Options	<i>policy-name</i> —Name of the policy that filters neighbor IP addresses.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring Interface-Level PIM Neighbor Policies

pim

```

Syntax  pim {
        disable;
        assert-timeout seconds;
        dense-groups {
            addresses;
        }
        dr-election-on-p2p;
        export;
        family (inet | inet6) {
            disable;
        }
        graceful-restart {
            disable;
            restart-duration seconds;
        }
        import [ policy-names ];
        interface interface-name {
            accept-remote-source;
            disable;
            bfd-liveness-detection {
                authentication {
                    algorithm algorithm-name;
                    key-chain key-chain-name;
                    loose-check;
                }
                detection-time {
                    threshold milliseconds;
                }
                minimum-interval milliseconds;
                minimum-receive-interval milliseconds;
                multiplier number;
                version (0 | 1 | automatic);
            }
            family (inet | inet6) {
                disable;
            }
            hello-interval seconds;
            mode (dense | sparse | sparse-dense);
            neighbor-policy [ policy-names ];
            override-interval milliseconds;
            priority number;
            propagation-delay milliseconds;
            reset-tracking-bit;
            version version;
        }
        join-load-balance;
        join-prune-timeout;
        nonstop-routing;
        override-interval milliseconds;
        propagation-delay milliseconds;
        reset-tracking-bit;
        rib-group group-name;
    }

```

```
rp {
  auto-rp {
    (announce | discovery | mapping);
    (mapping-agent-election | no-mapping-agent-election);
  }
  bootstrap {
    family (inet | inet6) {
      export [ policy-names ];
      import [ policy-names ];
      priority number;
    }
  }
  bootstrap-import [ policy-names ];
  bootstrap-export [ policy-names ];
  bootstrap-priority number;
  dr-register-policy [ policy-names ];
  embedded-rp {
    group-ranges {
      destination-ip-prefix </prefix-length>;
    }
    maximum-rps limit;
  }
  local {
    family (inet | inet6) {
      address address;
      anycast-pim {
        rp-set {
          address address <forward-msdp-sa>;
        }
        disable;
        local-address address;
      }
      group-ranges {
        destination-ip-prefix </prefix-length>;
      }
      hold-time seconds;
      priority number;
    }
  }
  rp-register-policy [ policy-names ];
  spt-threshold {
    infinity [ policy-names ];
  }
  static {
    address address {
      version version;
      group-ranges {
        destination-ip-prefix </prefix-length>;
      }
    }
  }
}
rpf-selection {
  group group-address {
    source source-address {
      next-hop next-hop-address;
    }
  }
}
```

```

    }
    wildcard-source {
        next-hop next-hop-address;
    }
}
prefix-list prefix-list-addresses {
    source source-address {
        next-hop next-hop-address;
    }
    wildcard-source {
        next-hop next-hop-address;
    }
}
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
tunnel-devices [ mt-fpc/pic/port ];
}

```

Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols], [edit protocols], [edit routing-instances <i>routing-instance-name</i> protocols]
Release Information	Statement introduced before Junos OS Release 7.4. family statement introduced in Junos OS Release 9.6. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Enable PIM on the routing device. The statements are explained separately.
Default	PIM is disabled on the routing device.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring PIM Dense Mode Properties Configuring PIM Sparse-Dense Mode Properties

priority (Bootstrap)

Syntax	<code>priority <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp bootstrap (inet inet6)], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap (inet inet6)], [edit protocols pim rp bootstrap (inet inet6)], [edit routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap (inet inet6)]
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the routing device's likelihood to be elected as the bootstrap router.
Options	<i>number</i> —Routing device's priority for becoming the bootstrap router. A higher value corresponds to a higher priority. Range: 0 through a 32-bit number Default: 0 (The routing device has the least likelihood of becoming the bootstrap router and sends packets with a priority of 0.)
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring PIM Bootstrap Properties for IPv4Configuring PIM Bootstrap Properties for IPv4 or IPv6bootstrap-priority on page 49

priority (PIM Interfaces)

Syntax	<code>priority <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols <code>pim interface <i>interface-name</i></code>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols <code>pim interface <i>interface-name</i></code>], [edit protocols <code>pim interface <i>interface-name</i></code>], [edit routing-instances <i>routing-instance-name</i> protocols <code>pim interface <i>interface-name</i></code>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the routing device's likelihood to be elected as the designated router.
Options	<i>number</i> —Routing device's priority for becoming the designated router. A higher value corresponds to a higher priority. Range: 0 through a 32-bit number Default: 0 (The routing device has the least likelihood of becoming the designated router.)
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring Interface Priority for the PIM Designated Router Selection

priority (PIM RPs)

Syntax	<code>priority <i>number</i>;</code>
Hierarchy Level	[edit protocols <code>pim rp local family</code> (inet inet6)], [edit routing-instances <i>routing-instance-name</i> protocols <code>pim rp local family</code> (inet inet6)]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure this routing device's priority for becoming an RP. The bootstrap router uses this field when selecting the list of candidate RPs to send in the bootstrap message. A smaller number increases the likelihood that the routing device becomes the RP for local multicast groups. A priority value of 0 means that bootstrap router can override the group range being advertised by the candidate RP.
Options	<i>number</i> —Routing device's priority for becoming an RP. A lower value corresponds to a higher priority. Range: 0 through 255 Default: 1
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring Local PIM RPs


promiscuous-mode

Syntax	<code>promiscuous-mode;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp <code>interface interface-name</code>], [edit protocols igmp <code>interface interface-name</code>]
Release Information	Statement introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify that the interface accepts IGMP reports from hosts on any subnetwork.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Accepting IGMP Messages from Remote Subnetworks

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 OS 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	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• [edit protocols] Configuration Statement Hierarchy on page 35• Example: Configuring Multicast VLAN Registration on EX Series Switches on page 20• Configuring Multicast VLAN Registration (CLI Procedure) on page 30


query-interval

Syntax	<code>query-interval seconds;</code>
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-name</i>]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches. Statement deprecated in Junos OS Release 9.4 for EX Series switches.
	<div> NOTE: This statement has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use.</div>
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 Documentation	<ul style="list-style-type: none">• Example: Configuring IGMP Snooping on EX Series Switches on page 17• Configuring IGMP Snooping (CLI Procedure) on page 25

query-interval

Syntax	query-interval <i>seconds</i> ;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp], [edit protocols igmp]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify how often the querier router sends general host-query messages.
Options	<i>seconds</i> —Time interval. Range: 1 through 1024 Default: 125 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Modifying the IGMP Host-Query Message Interval• query-last-member-interval on page 89• query-response-interval on page 91


query-last-member-interval

Syntax	query-last-member-interval <i>seconds</i> ;
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-name</i>]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches. Statement deprecated in Junos OS Release 9.4 for EX Series switches.
	<div> NOTE: This statement has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use.</div>
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 Documentation	<ul style="list-style-type: none">• Example: Configuring IGMP Snooping on EX Series Switches on page 17• Configuring IGMP Snooping (CLI Procedure) on page 25

query-last-member-interval

Syntax	query-last-member-interval <i>seconds</i> ;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp], [edit protocols igmp]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify how often the querier router sends group-specific query messages.
Options	seconds —Time interval, in fractions of a second or seconds. Range: 0.1 through 0.9, then in 1-second intervals 1 through 999999 Default: 1 second
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Modifying the IGMP Last-Member Query Interval• query-interval on page 87• query-response-interval on page 91

query-response-interval

Syntax	query-response-interval <i>seconds</i> ;
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-name</i>]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches. Statement deprecated in Junos OS Release 9.4 for EX Series switches.
	<div> NOTE: This statement has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use.</div>
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 Documentation	<ul style="list-style-type: none">• Example: Configuring IGMP Snooping on EX Series Switches on page 17• Configuring IGMP Snooping (CLI Procedure) on page 25

query-response-interval

Syntax	<code>query-response-interval <i>seconds</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp], [edit protocols igmp]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify how long the querier router waits to receive a response to a host-query message from a host.
Options	<i>seconds</i> —The query response interval must be less than the query interval. Range: 1 through 1024 Default: 10 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Modifying the IGMP Query Response Interval query-interval on page 87 query-last-member-interval on page 89

receiver

Syntax	<pre> receiver { source-vlans <i>vlan-list</i>; install; } </pre>
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-number</i> data-forwarding]
Release Information	Statement introduced in Junos OS 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 Documentation	<ul style="list-style-type: none"> [edit protocols] Configuration Statement Hierarchy on page 35 Example: Configuring Multicast VLAN Registration on EX Series Switches on page 20 Configuring Multicast VLAN Registration (CLI Procedure) on page 30

restart-duration

Syntax	<code>restart-duration <i>seconds</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim graceful-restart], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim graceful-restart], [edit protocols pim graceful-restart], [edit routing-instances <i>routing-instance-name</i> protocols pim graceful-restart]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the duration of the graceful restart interval.
Options	<i>seconds</i> —Time the routing device waits (in seconds) to complete PIM sparse mode graceful restart. Range: 30 through 300 Default: 60
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring PIM Sparse Mode Graceful Restart

rib-group

Syntax	<code>rib-group <i>group-name</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Associate a routing table group with PIM.
Options	<i>group-name</i> —Name of the routing table group. The name must be one that you defined with the rib-group statement at the [edit routing-options] hierarchy level.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Example: Configuring a Dedicated PIM RPF Routing Table

robust-count

Syntax	<code>robust-count <i>number</i>;</code>
Hierarchy Level	<code>[edit protocols igmp-snooping vlan <i>vlan-id</i> <i>vlan-name</i>]</code>
Release Information	Statement introduced in Junos OS 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 Documentation	<ul style="list-style-type: none"> • Example: Configuring IGMP Snooping on EX Series Switches on page 17 • Configuring IGMP Snooping (CLI Procedure) on page 25

robust-count

Syntax	<code>robust-count <i>number</i>;</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> protocols igmp],</code> <code>[edit protocols igmp]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Tune the expected packet loss on a subnet. This factor is used to calculate the group member interval, other querier present interval, and last-member query count.
Options	<i>number</i> —Robustness variable. Range: 2 through 10 Default: 2
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Modifying the IGMP Robustness Variable

rp

```

Syntax  rp {
    auto-rp {
        (announce | discovery | mapping);
        (mapping-agent-election | no-mapping-agent-election);
    }
    bootstrap {
        family (inet | inet6) {
            export [ policy-names ];
            import [ policy-names ];
            priority number;
        }
    }
    bootstrap-export [ policy-names ];
    bootstrap-import [ policy-names ];
    bootstrap-priority number;
    dr-register-policy [ policy-names ];
    embedded-rp {
        group-ranges {
            destination-ip-prefix </prefix-length>;
        }
        maximum-rps limit;
    }
    local {
        family (inet | inet6) {
            disable;
            address address;
            anycast-pim {
                rp-set {
                    address address <forward-msdp-sa>;
                }
                local-address address;
            }
            group-ranges {
                destination-ip-prefix </prefix-length>;
            }
            hold-time seconds;
            priority number;
        }
    }
    rp-register-policy [ policy-names ];
    static {
        address address {
            version version;
            group-ranges {
                destination-ip-prefix </prefix-length>;
            }
        }
    }
}

```

Hierarchy Level [edit logical-systems *logical-system-name* protocols *pim*],

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols [pim](#)],
 [edit protocols [pim](#)],
 [edit routing-instances *routing-instance-name* protocols [pim](#)]

Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the routing device as an actual or potential RP. A routing device can be an RP for more than one group. The remaining statements are explained separately.
Default	If you do not include the rp statement, the routing device can never become the RP.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Understanding PIM Sparse Mode

[rp-register-policy](#)

Syntax	rp-register-policy [<i>policy-names</i>];
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp], [edit protocols pim rp], [edit routing-instances <i>routing-instance-name</i> protocols pim rp]
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Apply one or more policies to control incoming PIM register messages.
Options	<i>policy-names</i> —Name of one or more import policies.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring Register Message Filters on a PIM RP and DR dr-register-policy on page 54

rp-set

Syntax	<pre>rp-set { address address <forward-msdp-sa>; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim local family (inet inet6) anycast-pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim local family (inet inet6) anycast-pim], [edit protocols pim local family (inet inet6) anycast-pim], [edit routing-instances <i>routing-instance-name</i> protocols pim local family (inet inet6) anycast-pim]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure a set of rendezvous point (RP) addresses for anycast RP. You can configure up to 15 RPs. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring PIM Anycast With or Without MSDP

source

Syntax	<pre>source { groups group-prefix; }</pre>
Hierarchy Level	[edit protocols igmp-snooping vlan <i>vlan-number</i> data-forwarding]
Release Information	Statement introduced in Junos OS 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 Documentation	<ul style="list-style-type: none">• [edit protocols] Configuration Statement Hierarchy on page 35• Example: Configuring Multicast VLAN Registration on EX Series Switches on page 20• Configuring Multicast VLAN Registration (CLI Procedure) on page 30

source

Syntax	source <i>ip-address</i> { source-count <i>number</i> ; source-increment <i>increment</i> ; }
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp <i>interface interface-name</i> static group <i>multicast-group-address</i>], [edit protocols igmp <i>interface interface-name</i> static group <i>multicast-group-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the IP version 4 (IPv4) unicast source address for the multicast group being statically configured on an interface.
Options	<i>ip-address</i> —IPv4 unicast address. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Enabling IGMP Static Group Membership

source-vlans

Syntax	source-vlans <i>vlan-list</i> ;
Hierarchy Level	[edit protocols <i>igmp-snooping</i> vlan <i>vlan-id</i> <i>vlan-number</i> data-forwarding receiver]
Release Information	Statement introduced in Junos OS 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 Documentation	<ul style="list-style-type: none"> [edit protocols] Configuration Statement Hierarchy on page 35 Example: Configuring Multicast VLAN Registration on EX Series Switches on page 20 Configuring Multicast VLAN Registration (CLI Procedure) on page 30

spt-threshold

Syntax	<code>spt-threshold { infinfinity [<i>policy-names</i>]; }</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim]
Release Information	Statement introduced in Junos OS Release 8.0. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Set the SPT threshold to infinity for a source-group address pair. Last-hop multicast routing devices running PIM sparse mode can forward the same stream of multicast packets onto the same LAN through an RPT rooted at the RP or an SPT rooted at the source. By default, last-hop routing devices transition to a direct SPT to the source. You can configure this routing device to set the SPT transition value to infinity to prevent this transition for any source-group address pair.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring the PIM SPT Threshold Policy

ssm-map

Syntax	<code>ssm-map <i>ssm-map-name</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Apply an SSM map to an IGMP interface.
Options	<i>ssm-map-name</i> —Name of SSM map.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring SSM Mapping

static

Syntax	<pre>static { address address { group-ranges { destination-ip-prefix</prefix-length>; } version version; } }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp],</p> <p>[edit protocols pim rp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	<p>Configure static RP addresses. The default static RP address is 224.0.0.0/4. To configure other addresses, include one or more address statements. You can configure a static RP in a logical system only if the logical system is not directly connected to a source.</p> <p>For each static RP address, you can optionally specify the PIM version and the groups for which this address can be the RP. The default PIM version is version 1.</p> <p>The remaining statements are explained separately.</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 Documentation	<ul style="list-style-type: none"> Configuring the Static PIM RP Address on the Non-RP Routing Device

static (IGMP Snooping)

Syntax	<code>static { group ip-address; }</code>
Hierarchy Level	[edit protocols igmp-snooping vlan (<i>vlan-id</i> <i>vlan-name</i>) interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.1 for EX-series switches.
Description	Statically define multicast groups on an interface. The remaining statement is explained separately.
Default	No multicast groups are statically defined.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring IGMP Snooping on EX Series Switches on page 17• Configuring IGMP Snooping (CLI Procedure) on page 25

static

Syntax	<pre>static { group multicast-group-address { exclude; group-count <i>number</i>; group-increment <i>increment</i>; source ip-address { source-count <i>number</i>; source-increment <i>increment</i>; } } }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Test multicast forwarding on an interface without a receiver host. The remaining statements are explained separately.
Required Privilege Level	routing and trace—To view this statement in the configuration. routing-control and trace-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Enabling IGMP Static Group Membership

traceoptions

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i> <flag-modifier> <disable>; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure PIM tracing options. To specify more than one tracing operation, include multiple flag statements.
Default	The default PIM trace options are those inherited from the routing protocol's traceoptions statement included at the [edit routing-options] hierarchy level.
Options	<p>disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.</p> <p>file <i>filename</i>—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. We recommend that you place tracing output in the pim-log file.</p> <p>files <i>number</i>—(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. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you must also include the size statement to specify the maximum file size.</p> <p>Range: 2 through 1000 files Default: 2 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.</p> <p>PIM Tracing Flags</p> <ul style="list-style-type: none">• assert—Assert messages• bootstrap—Bootstrap messages• cache—Packets in the PIM sparse mode routing cache

- **graft**—Graft and graft acknowledgment messages
- **hello**—Hello packets
- **join**—Join messages
- **mt**—Multicast tunnel messages
- **nsr-synchronization**—Nonstop active routing (NSR) synchronization messages
- **packets**—All PIM packets
- **prune**—Prune messages
- **register**—Register and register stop messages
- **rp**—Candidate RP advertisements
- **all**—All tracing operations
- **general**—A combination of the **normal** and **route** trace operations
- **normal**—All normal operations

Default: If you do not specify this option, only unusual or abnormal operations are traced.

- **policy**—Policy operations and actions
- **route**—Routing table changes
- **state**—State transitions
- **task**—Interface transactions and processing
- **timer**—Timer usage

flag-modifier—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

- **detail**—Detailed trace information
- **receive**—Packets being received
- **send**—Packets being transmitted

no-stamp—(Optional) Do not place timestamp information at the beginning of each line in the trace file.

Default: If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

no-world-readable—(Optional) Do not allow users to read the log file.

replace—(Optional) Replace an existing trace file if there is one.

Default: If you do not include this option, tracing output is appended to an existing trace 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 this size, it is renamed **trace-file.0**. When **trace-file** again reaches this size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you must also include the **files** statement to specify the maximum number of trace files.

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

Range: 0 KB through the maximum file size supported on your system

Default: 1 MB

world-readable—(Optional) Allow any user to read the log file.

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

Related Documentation	<ul style="list-style-type: none">• Configuring PIM Trace Options• Tracing DVMRP Protocol Traffic• Tracing MSDP Protocol Traffic• Configuring PIM Trace Options
------------------------------	--

traceoptions

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable> <match <i>regex</i>>; flag <i>flag</i> (detail disable receive send); } </pre>
Hierarchy Level	[edit protocols igmp-snooping]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Define tracing operations for IGMP snooping.
Default	The traceoptions feature is disabled by default.
Options	<p>file <i>filename</i> —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.</p> <p>files <i>number</i> —(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.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i> —Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> • 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 Documentation	• Example: Configuring IGMP Snooping on EX Series Switches on page 17
	• Configuring IGMP Snooping (CLI Procedure) on page 25

traceoptions

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i> <flag-modifier> <disable>; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp], [edit protocols igmp]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Configure IGMP tracing options.</p> <p>To specify more than one tracing operation, include multiple flag statements.</p> <p>To trace the paths of multicast packets, use the mtrace command.</p>
Default	The default IGMP trace options are those inherited from the routing protocols traceoptions statement included at the [edit routing-options] hierarchy level.
Options	<p>disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.</p> <p>file <i>filename</i>—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. We recommend that you place tracing output in the file igmp-log.</p> <p>files <i>number</i>—(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. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you must also include the size statement to specify the maximum file size.</p> <p>Range: 2 through 1000 files</p> <p>Default: 2 files</p> <p>flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.</p> <p>IGMP Tracing Flags</p> <ul style="list-style-type: none"> • leave—Leave group messages (for IGMP version 2 only). • mtrace—Mtrace packets. Use the mtrace command to troubleshoot the software. • packets—All IGMP packets.

- **query**—IGMP membership query messages, including general and group-specific queries.
- **report**—Membership report messages.

Global Tracing Flags

- **all**—All tracing operations
- **general**—A combination of the **normal** and **route** trace operations
- **normal**—All normal operations

Default: If you do not specify this option, only unusual or abnormal operations are traced.

- **policy**—Policy operations and actions
- **route**—Routing table changes
- **state**—State transitions
- **task**—Interface transactions and processing
- **timer**—Timer usage

flag-modifier—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

- **detail**—Detailed trace information
- **receive**—Packets being received
- **send**—Packets being transmitted

no-stamp—(Optional) Do not place timestamp information at the beginning of each line in the trace file.

Default: If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

no-world-readable—(Optional) Do not allow users to read the log file.

replace—(Optional) Replace an existing trace file if there is one.

Default: If you do not include this option, tracing output is appended to an existing trace 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 this size, it is renamed **trace-file.0**. When **trace-file** again reaches this size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you must also include the **files** statement to specify the maximum number of trace files.

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

Range: 10 KB through the maximum file size supported on your system

Default: 1 MB

world-readable—(Optional) Allow any user to read the log file.

Required Privilege Level	routing and trace—To view this statement in the configuration.
	routing-control and trace-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Tracing IGMP Protocol Traffic

version

Syntax	<code>version <i>version</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the version of IGMP.
Options	<p>version—IGMP version number.</p> <p>Range: 1, 2, or 3</p> <p>Default: IGMP version 2</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 Documentation	<ul style="list-style-type: none"> Changing the IGMP Version

version (PIM)

Syntax	<code>version version;</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> protocols pim interface <i>interface-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> protocols pim rp static address <i>address</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols</code> <code> pim interface <i>interface-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols</code> <code> pim rp static address <i>address</i>],</code> <code>[edit protocols pim interface <i>interface-name</i>],</code> <code>[edit protocols pim rp static address <i>address</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols pim rp static address <i>address</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the version of PIM.
Options	version —PIM version number. Range: 1 or 2 Default: PIMv1 for rendezvous point (RP) mode (at the <code>[edit protocols pim rp static address <i>address</i>]</code> hierarchy level). PIMv2 for interface mode (at the <code>[edit protocols pim interface <i>interface-name</i>]</code> hierarchy level).
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Enabling PIM Sparse Mode• Configuring PIM Dense Mode Properties• Configuring PIM Sparse-Dense Mode Properties

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 (IGMP Snooping) {
                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 OS Release 9.1 for EX Series switches.
Statement updated with enhanced ? (CLI completion feature) functionality in Junos OS 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 vlans 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 OS, and you should not configure them.

vlan-name—Name of a VLAN.

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

Related Documentation	<ul style="list-style-type: none">• Configuring IGMP Snooping (CLI Procedure) on page 25• IGMP Snooping on EX Series Switches Overview on page 3
------------------------------	---

CHAPTER 6

Operational Commands for IGMP Snooping and Multicast

clear igmp membership

Syntax	clear igmp membership <group <i>address-range</i> > <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	clear igmp membership <group <i>address-range</i> > <interface <i>interface-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Clear Internet Group Management Protocol (IGMP) group members.
Options	<p>none—Clear all IGMP members on all interfaces and for all address ranges.</p> <p>group <i>address-range</i>—(Optional) Clear all IGMP members that are in a particular address range. An example of a range is 224.2/16. If you omit the destination prefix length, the default is /32.</p> <p>interface <i>interface-name</i>—(Optional) Clear all IGMP group members on an interface.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show igmp group on page 141 • show igmp interface on page 145
List of Sample Output	clear igmp membership on page 114 clear igmp membership interface on page 115 clear igmp membership group on page 115
Output Fields	See show igmp group for an explanation of output fields.

Sample Output

clear igmp membership The following sample output displays IGMP group information before and after the **clear igmp membership** command is entered:

```

user@host> show igmp group
Interface      Group           Last Reported   Timeout
so-0/0/0       224.2.127.253   10.1.128.1      186
so-0/0/0       224.2.127.254   10.1.128.1      186
so-0/0/0       239.255.255.255 10.1.128.1      187
so-0/0/0       224.1.127.255   10.1.128.1      188
local          224.0.0.6       (null)          0
local          224.0.0.5       (null)          0

```

```

local 224.2.127.254 (null) 0
local 239.255.255.255 (null) 0
local 224.0.0.2 (null) 0
local 224.0.0.13 (null) 0

```

```

user@host> clear igmp membership
Clearing Group Membership Info for so-0/0/0
Clearing Group Membership Info for so-1/0/0
Clearing Group Membership Info for so-2/0/0

```

```

user@host> show igmp group
Interface      Group      Last Reported  Timeout
local         224.0.0.6   (null)         0
local         224.0.0.5   (null)         0
local         224.2.127.254 (null)         0
local         239.255.255.255 (null)         0
local         224.0.0.2   (null)         0
local         224.0.0.13   (null)         0

```

clear igmp membership interface

The following sample output displays IGMP group information before and after the **clear igmp membership interface** command is issued:

```

user@host> show igmp group
Interface      Group      Last Reported  Timeout
so-0/0/0      224.2.127.253 10.1.128.1    210
so-0/0/0      239.255.255.255 10.1.128.1    210
so-0/0/0      224.1.127.255 10.1.128.1    215
so-0/0/0      224.2.127.254 10.1.128.1    216
local         224.0.0.6   (null)         0
local         224.0.0.5   (null)         0
local         224.2.127.254 (null)         0
local         239.255.255.255 (null)         0
local         224.0.0.2   (null)         0
local         224.0.0.13   (null)         0

```

```

user@host> clear igmp membership interface so-0/0/0
Clearing Group Membership Info for so-0/0/0

```

```

user@host> show igmp group
Interface      Group      Last Reported  Timeout
local         224.0.0.6   (null)         0
local         224.0.0.5   (null)         0
local         224.2.127.254 (null)         0
local         239.255.255.255 (null)         0
local         224.0.0.2   (null)         0
local         224.0.0.13   (null)         0

```

clear igmp membership group

The following sample output displays IGMP group information before and after the **clear igmp membership group** command is entered:

```

user@host> show igmp group
Interface      Group      Last Reported  Timeout
so-0/0/0      224.2.127.253 10.1.128.1    210
so-0/0/0      239.255.255.255 10.1.128.1    210
so-0/0/0      224.1.127.255 10.1.128.1    215
so-0/0/0      224.2.127.254 10.1.128.1    216
local         224.0.0.6   (null)         0

```

local	224.0.0.5	(null)	0
local	224.2.127.254	(null)	0
local	239.255.255.255	(null)	0
local	224.0.0.2	(null)	0
local	224.0.0.13	(null)	0

```
user@host> clear igmp membership group 239.225/16
Clearing Group Membership Range 239.225.0.0/16 on so-0/0/0
Clearing Group Membership Range 239.225.0.0/16 on so-1/0/0
Clearing Group Membership Range 239.225.0.0/16 on so-2/0/0
```



```
user@host> show igmp group
```

Interface	Group	Last Reported	Timeout
so-0/0/0	224.1.127.255	10.1.128.1	231
so-0/0/0	224.2.127.254	10.1.128.1	233
so-0/0/0	224.2.127.253	10.1.128.1	236
local	224.0.0.6	(null)	0
local	224.0.0.5	(null)	0
local	224.2.127.254	(null)	0
local	239.255.255.255	(null)	0
local	224.0.0.2	(null)	0
local	224.0.0.13	(null)	0

clear igmp statistics

Syntax	clear igmp statistics <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	clear igmp statistics <interface <i>interface-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Clear Internet Group Management Protocol (IGMP) statistics.
Options	none—Clear IGMP statistics on all interfaces. interface <i>interface-name</i> —(Optional) Clear IGMP statistics for the specified interface only. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show igmp statistics on page 148
List of Sample Output	clear igmp statistics on page 118
Output Fields	See show igmp statistics for an explanation of output fields.

Sample Output

clear igmp statistics The following sample output displays IGMP statistics information before and after the **clear igmp statistics** command is entered:

```

user@host> show igmp statistics
IGMP packet statistics for all interfaces
IGMP Message type      Received      Sent  Rx errors
Membership Query        8883         459      0
V1 Membership Report    0            0        0
DVMRP                   19784        35476     0
PIM V1                  18310         0        0
Cisco Trace             0            0        0
V2 Membership Report    0            0        0
Group Leave             0            0        0
Mtrace Response         0            0        0
Mtrace Request          0            0        0
Domain Wide Report      0            0        0
V3 Membership Report    0            0        0
Other Unknown types     0            0        0
IGMP v3 unsupported type 0            0        0
IGMP v3 source required for SSM 0
IGMP v3 mode not applicable for SSM 0

```

```
IGMP Global Statistics
Bad Length          0
Bad Checksum        0
Bad Receive If      0
Rx non-local        1227
```

```
user@host> clear igmp statistics
```

```
user@host> show igmp statistics
```

```
IGMP packet statistics for all interfaces
IGMP Message type      Received      Sent  Rx errors
Membership Query        0           0      0
V1 Membership Report    0           0      0
DVMRP                   0           0      0
PIM V1                  0           0      0
Cisco Trace             0           0      0
V2 Membership Report    0           0      0
Group Leave             0           0      0
Mtrace Response         0           0      0
Mtrace Request          0           0      0
Domain Wide Report      0           0      0
V3 Membership Report     0           0      0
Other Unknown types     0           0      0
IGMP v3 unsupported type 0           0      0
IGMP v3 source required for SSM 0           0      0
IGMP v3 mode not applicable for SSM 0           0      0
IGMP Global Statistics
Bad Length              0
Bad Checksum            0
Bad Receive If          0
Rx non-local            0
```

clear igmp-snooping membership

Syntax	clear igmp-snooping membership <vlan <i>vlan-id</i> <i>vlan-name</i>>
Release Information	Command introduced in Junos OS 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 Documentation	<ul style="list-style-type: none"> • show igmp-snooping membership on page 151
List of Sample Output	clear igmp-snooping membership on page 120

Sample Output

```
clear igmp-snooping membership
user@switch> clear igmp-snooping membership vlan employee-vlan
```

clear igmp-snooping statistics

Syntax	<code>clear igmp-snooping statistics</code>
Release Information	Command introduced in Junos OS Release 9.1 for EX Series switches.
Description	Clear IGMP snooping statistics.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show igmp-snooping statistics on page 155
List of Sample Output	clear igmp-snooping statistics on page 121

Sample Output

<code>clear igmp-snooping statistics</code>	<code>user@switch> clear igmp-snooping statistics</code>
---	---

clear multicast bandwidth-admission

Syntax	<pre>clear multicast bandwidth-admission <group <i>group-address</i>> <inet inet6> <instance <i>instance-name</i>> <interface <i>interface-name</i>> <source <i>source-address</i>></pre>
Release Information	Command introduced in Junos OS Release 8.3. Command introduced in Junos OS Release 9.0 for EX Series switches. inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Description	Reapply IP multicast bandwidth admissions.
Options	<p>none—Reapply multicast bandwidth admissions for all IPv4 forwarding entries in the master routing instance.</p> <p><i>group group-address</i>—(Optional) Reapply multicast bandwidth admissions for the specified group.</p> <p>inet—(Optional) Reapply multicast bandwidth admission settings for IPv4 flows.</p> <p>inet6—(Optional) Reapply multicast bandwidth admission settings for IPv6 flows.</p> <p>instance <i>instance-name</i>—(Optional) Reapply multicast bandwidth admission settings for the specified instance. If you do not specify an instance, the command applies to the master routing instance.</p> <p>interface <i>interface-name</i>—(Optional) Examines the corresponding outbound interface in the relevant entries and acts as follows:</p> <ul style="list-style-type: none">• If the interface is congested, and it was admitted previously, it is removed.• If the interface was rejected previously, the clear multicast bandwidth-admission command enables the interface to be admitted as long as enough bandwidth exists on the interface.• If you do not specify an interface, issuing the clear multicast bandwidth-admission command readmits any previously rejected interface for the relevant entries as long as enough bandwidth exists on the interface. <p>To manually reject previously admitted outbound interfaces, you must specify the interface.</p> <p><i>source source-address</i>—(Optional) Use with the group option to reapply multicast bandwidth admission settings for the specified (source, group) entry.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show multicast interface on page 161

List of Sample Output [clear multicast bandwidth-admission on page 123](#)

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

Sample Output

```
clear multicast user@host> clear multicast bandwidth-admission
bandwidth-admission
```

clear multicast scope

Syntax	clear multicast scope <inet inet6> <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	clear multicast scope <inet inet6> <interface <i>interface-name</i> >
Release Information	Command introduced in Junos OS Release 7.6. Command introduced in Junos OS Release 9.0 for EX Series switches. inet6 option introduced in Junos OS Release 10.0 for EX Series switches.
Description	Clear IP multicast scope statistics.
Options	none—(Same as logical-system all) Clear multicast scope statistics. inet—(Optional) Clear multicast scope statistics for IPv4 family addresses. inet6—(Optional) Clear multicast scope statistics for IPv6 family addresses. interface <i>interface-name</i> —(Optional) Clear multicast scope statistics on a specific interface. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show multicast scope on page 180
List of Sample Output	clear multicast scope on page 124
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear multicast scope user@host> clear multicast scope

clear multicast sessions

Syntax	clear multicast sessions <logical-system (all <i>logical-system-name</i>)> < <i>regular-expression</i> >
Syntax (EX Series Switch)	clear multicast sessions < <i>regular-expression</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Clear IP multicast sessions.
Options	<p>none—(Same as logical-system all) Clear multicast sessions.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> <p><i>regular-expression</i>—(Optional) Clear only multicast sessions that contain the specified regular expression.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show multicast sessions on page 182
List of Sample Output	clear multicast sessions on page 125
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear multicast sessions  user@host> clear multicast sessions
```

clear multicast statistics

Syntax	clear multicast statistics <inet inet6> <instance <i>instance-name</i> > <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	clear multicast statistics <inet inet6> <instance <i>instance-name</i> > <interface <i>interface-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Description	Clear IP multicast statistics.
Options	none—Clear multicast statistics for all supported address families on all interfaces. inet—(Optional) Clear multicast statistics for IPv4 family addresses. inet6—(Optional) Clear multicast statistics for IPv6 family addresses. instance <i>instance-name</i> —(Optional) Clear multicast statistics for the specified instance. interface <i>interface-name</i> —(Optional) Clear multicast statistics on a specific interface. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show multicast statistics
List of Sample Output	clear multicast statistics on page 126
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear multicast statistics  user@host> clear multicast statistics
```

clear pim join

Syntax	clear pim join <group-address> <inet inet6> <instance instance-name> <logical-system (all logical-system-name)>
Syntax (EX Series Switch)	clear pim join <group-address> <inet inet6> <instance instance-name>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Description	Clear the Protocol Independent Multicast (PIM) join and prune states.
Options	<p>none—Clear the PIM join and prune states for all groups, family addresses, and instances.</p> <p>group-address—(Optional) Clear the PIM join and prune states for a group address.</p> <p>inet inet6—(Optional) Clear the PIM join and prune states for IPv4 or IPv6 family addresses, respectively.</p> <p>instance instance-name—(Optional) Clear the join and prune states for a specific PIM-enabled routing instance.</p> <p>logical-system (all logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Additional Information	The clear pim join command cannot be used to clear the PIM join and prune state on a backup Routing Engine when nonstop active routing is enabled.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show pim join on page 193
List of Sample Output	clear pim join on page 127
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear pim join user@host> clear pim join

clear pim register

Syntax	clear pim register <inet inet6> <instance <i>instance-name</i> > <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	clear pim register <inet inet6> <instance <i>instance-name</i> > <interface <i>interface-name</i> >
Release Information	Command introduced in Junos OS Release 7.6. Command introduced in Junos OS Release 9.0 for EX Series switches. inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Description	Clear Protocol Independent Multicast (PIM) register message counters.
Options	<p>none—Clear PIM register message counters for all family addresses, instances, and interfaces.</p> <p>inet inet6—(Optional) Clear PIM register message counters for IPv4 or IPv6 family addresses, respectively.</p> <p>instance <i>instance-name</i>—(Optional) Clear register message counters for a specific PIM-enabled routing instance.</p> <p>interface <i>interface-name</i>—(Optional) Clear PIM register message counters for a specific interface.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Additional Information	The clear pim register command cannot be used to clear the PIM register state on a backup Routing Engine when nonstop active routing is enabled.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show pim statistics on page 210
List of Sample Output	clear pim register on page 128
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear pim register user@host> clear pim register

clear pim statistics

Syntax	clear pim statistics <inet inet6> <instance <i>instance-name</i> > <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	clear pim statistics <inet inet6> <instance <i>instance-name</i> > <interface <i>interface-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Description	Clear Protocol Independent Multicast (PIM) statistics.
Options	<p>none—Clear PIM statistics for all family addresses, instances, and interfaces.</p> <p>inet inet6—(Optional) Clear PIM statistics for IPv4 or IPv6 family addresses, respectively.</p> <p>instance <i>instance-name</i>—(Optional) Clear statistics for a specific PIM-enabled routing instance.</p> <p>interface <i>interface-name</i>—(Optional) Clear PIM statistics for a specific interface.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Additional Information	The clear pim statistics command cannot be used to clear the PIM statistics on a backup Routing Engine when nonstop active routing is enabled.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show pim statistics on page 210
List of Sample Output	clear pim statistics on page 129
Output Fields	See show pim statistics for an explanation of output fields.

Sample Output

clear pim statistics The following sample output displays PIM statistics before and after the **clear pim statistics** command is entered:

```
user@host> show pim statistics
PIM statistics on all interfaces:
PIM Message type      Received      Sent  Rx errors
```

Hello	0	0	0
Register	0	0	0
Register Stop	0	0	0
Join Prune	0	0	0
Bootstrap	0	0	0
Assert	0	0	0
Graft	0	0	0
Graft Ack	0	0	0
Candidate RP	0	0	0
V1 Query	2111	4222	0
V1 Register	0	0	0
V1 Register Stop	0	0	0
V1 Join Prune	14200	13115	0
V1 RP Reachability	0	0	0
V1 Assert	0	0	0
V1 Graft	0	0	0
V1 Graft Ack	0	0	0
PIM statistics summary for all interfaces:			
Unknown type	0		
V1 Unknown type	0		
Unknown Version	0		
Neighbor unknown	0		
Bad Length	0		
Bad Checksum	0		
Bad Receive If	0		
Rx Intf disabled	2007		
Rx V1 Require V2	0		
Rx Register not RP	0		
RP Filtered Source	0		
Unknown Reg Stop	0		
Rx Join/Prune no state	1040		
Rx Graft/Graft Ack no state	0		
...			

```
user@host> clear pim statistics
```

```
user@host> show pim statistics
```

```
PIM statistics on all interfaces:
```

PIM Message type	Received	Sent	Rx errors
Hello	0	0	0
Register	0	0	0
Register Stop	0	0	0
Join Prune	0	0	0
Bootstrap	0	0	0
Assert	0	0	0
Graft	0	0	0
Graft Ack	0	0	0
Candidate RP	0	0	0
V1 Query	1	0	0
V1 Register	0	0	0
...			

mtrace

Syntax	<code>mtrace source</code> <code><routing-instance routing-instance-name></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display trace information about an IP multicast path.
Options	<code>source</code> —Source hostname or address. <code>routing-instance routing-instance-name</code> —(Optional) Trace a particular routing instance.
Additional Information	The mtrace command for multicast traffic is similar to the traceroute command used for unicast traffic. Unlike traceroute , mtrace traces traffic backwards, from the receiver to the source.
Required Privilege Level	view
List of Sample Output	mtrace source on page 132
Output Fields	Table 5 on page 131 describes the output fields for the mtrace command. Output fields are listed in the approximate order in which they appear.

Table 5: mtrace Output Fields

Field Name	Field Description
Mtrace from	IP address of the receiver.
to	IP address of the source.
via group	IP address of the multicast group (if any).
Querying full reverse path	Indicates the full reverse path query has begun.
number-of-hops	Number of hops from the source to the named router or switch.
router-name	Name of the router or switch for this hop.
address	Address of the router or switch for this hop.
protocol	Protocol used (for example, PIM).
Round trip time	Average round-trip time, in milliseconds (ms).
total ttl of	Time-to-live (TTL) threshold.

Sample Output

```
mtrace source user@host> mtrace 192.1.4.2
Mtrace from 192.1.4.2 to 192.1.1.2 via group 0.0.0.0
Querying full reverse path... * *
  0 routerA.lab.mycompany.net (192.1.1.2)
-1 routerB.lab.mycompany.net (192.1.2.2) PIM thresh^ 1
-2 routerC.lab.mycompany.net (192.1.3.2) PIM thresh^ 1
-3 hostA.lab.mycompany.net (192.1.4.2)
Round trip time 2 ms; total ttl of 2 required.
```


mtrace from-source

Syntax `mtrace from-source source source`
`<brief | detail>`
`<extra-hops extra-hops>`
`<group group>`
`<interval interval>`
`<loop>`
`<max-hops max-hops>`
`<max-queries max-queries>`
`<multicast-response | unicast-response>`
`<no-resolve>`
`<no-router-alert>`
`<response response>`
`<routing-instance routing-instance-name>`
`<tll ttl>`
`<wait-time wait-time>`

Release Information Command introduced before Junos OS Release 7.4.
 Command introduced in Junos OS Release 9.0 for EX Series switches.

Description Display trace information about an IP multicast path from a source to this router or switch. If you specify a group address with this command, the Junos OS returns additional information, such as packet rates and losses.

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

`extra-hops extra-hops`—(Optional) Number of hops to take after reaching a nonresponsive router. You can specify a number between **0** and **255**.

`group group`—(Optional) Group address for which to trace the path. The default group address is **0.0.0.0**.

`interval interval`—(Optional) Number of seconds to wait before gathering statistics again. The default value is **10** seconds.

`loop`—(Optional) Loop indefinitely, displaying rate and loss statistics.

`max-hops max-hops`—(Optional) Maximum hops to trace toward source. The range of values is **0** through **255**. The default value is **32** hops.

`max-queries max-queries`—(Optional) Maximum number of query attempts for any hop. The range of values is **1** through **32**. The default is **3**.

`multicast-response`—(Optional) Always request the response using multicast.

`no-resolve`—(Optional) Do not attempt to display addresses symbolically.

`no-router-alert`—(Optional) Do not use the router-alert IP option.

`response response`—(Optional) Send trace response to a host or multicast address.

`routing-instance routing-instance-name`—(Optional) Trace a particular routing instance.

source *source*—Source hostname or address.

ttl *tll*—(Optional) IP time-to-live (TTL) value. You can specify a number between 0 and 255. Local queries to the multicast group use a value of 1. Otherwise, the default value is 127.

unicast-response—(Optional) Always request the response using unicast.

wait-time *wait-time*—(Optional) Number of seconds to wait for a response. The default value is 3.

Required Privilege Level view

List of Sample Output [mtrace from-source on page 135](#)

Output Fields [Table 6 on page 134](#) describes the output fields for the **mtrace from-source** command. Output fields are listed in the approximate order in which they appear.

Table 6: mtrace from-source Output Fields

Field Name	Field Description
Mtrace from	IP address of the receiver.
to	IP address of the source.
via group	IP address of the multicast group (if any).
Querying full reverse path	Indicates the full reverse path query has begun.
<i>number-of-hops</i>	Number of hops from the source to the named router or switch.
<i>router-name</i>	Name of the router or switch for this hop.
<i>address</i>	Address of the router or switch for this hop.
<i>protocol</i>	Protocol used (for example, PIM).
Round trip time	Average round-trip time, in milliseconds (ms).
total ttl of	Time-to-live (TTL) threshold.
source	Source address.
Response Dest	Response destination address.
Overall	Average packet rate for all traffic at each hop.
Packet Statistics for Traffic From	Number of packets lost, number of packets sent, percentage of packets lost, and average packet rate at each hop.

Table 6: mtrace from-source Output Fields (*continued*)

Field Name	Field Description
Receiver	IP address receiving the multicast.
Query source	IP address sending the mtrace query.

Sample Output

```

mtrace from-source user@host> mtrace from-source source 192.1.4.2 group 225.1.1.1
Mtrace from 192.1.4.2 to 192.1.1.2 via group 225.1.1.1
Querying full reverse path... * *
  0 routerA.lab.mycompany.net (192.1.1.2)
 -1 routerB.lab.mycompany.net (192.1.2.2) PIM thresh^ 1
 -2 routerC.lab.mycompany.net (192.1.3.2) PIM thresh^ 1
 -3 hostA.lab.mycompany.net (192.1.4.2)
Round trip time 2 ms; total ttl of 2 required.

Waiting to accumulate statistics...Results after 10 seconds:

Source      Response Dest    Overall    Packet Statistics For Traffic From
192.1.4.2 192.1.1.2 Packet    192.1.4.2 To 225.1.1.1
  v      _/ rtt    2 ms    Rate    Lost/Sent = Pct Rate
192.1.2.1
192.1.3.2 routerC.lab.mycompany.net
  v      ^    ttl    2          0/0    = --    0 pps
192.1.4.1
192.1.2.2 routerB.lab.mycompany.net
  v      \_    ttl    3          ?/0          0 pps
192.1.1.2 192.1.1.2
Receiver      Query Source

```

mtrace monitor

Syntax	mtrace monitor
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Listen passively for IP multicast responses. To exit mtrace monitor , type Ctrl+c.
Options	none—Trace the master instance.
Required Privilege Level	view
List of Sample Output	mtrace monitor on page 137
Output Fields	Table 7 on page 136 describes the output fields for the mtrace monitor command. Output fields are listed in the approximate order in which they appear.

Table 7: mtrace monitor Output Fields

Field Name	Field Description
Mtrace query at	Date and time of the query.
by	Address of the host issuing the query.
resp to	Response destination.
qid	Query ID number.
packet from...to	IP address of the query source and default group destination.
from...to	IP address of the multicast source and the response address.
via group	IP address of the group to trace.
mxhop	Maximum hop setting.

Sample Output

```
mtrace monitor user@host> mtrace monitor
Mtrace query at Oct 22 13:36:14 by 192.1.3.2, resp to 224.0.1.32, qid 74a5b8
packet from 192.1.3.2 to 224.0.0.2
from 192.1.3.2 to 192.1.3.38 via group 224.1.1.1 (mxhop=60)

Mtrace query at Oct 22 13:36:17 by 192.1.3.2, resp to 224.0.1.32, qid 1d07ba
packet from 192.1.3.2 to 224.0.0.2
from 192.1.3.2 to 192.1.3.38 via group 224.1.1.1 (mxhop=60)

Mtrace query at Oct 22 13:36:20 by 192.1.3.2, resp to same, qid 2feald
packet from 192.1.3.2 to 224.0.0.2
from 192.1.3.2 to 192.1.3.38 via group 224.1.1.1 (mxhop=60)

Mtrace query at Oct 22 13:36:30 by 192.1.3.2, resp to same, qid 7c88ad
packet from 192.1.3.2 to 224.0.0.2
from 192.1.3.2 to 192.1.3.38 via group 224.1.1.1 (mxhop=60)
```

mtrace to-gateway

Syntax mtrace to-gateway gateway gateway
 <brief | detail>
 <extra-hops *extra-hops*>
 <group *group*>
 <interface *interface-name*>
 <interval *interval*>
 <loop>
 <max-hops *max-hops*>
 <max-queries *max-queries*>
 <multicast-response | unicast-response>
 <no-resolve>
 <no-router-alert>
 <response *response*>
 <routing-instance *routing-instance-name*>
 <tll *tll*>
 <unicast-response>
 <wait-time *wait-time*>

Release Information Command introduced before Junos OS Release 7.4.
 Command introduced in Junos OS Release 9.0 for EX Series switches.

Description Display trace information about a multicast path from this router or switch to a gateway router or switch.

Options gateway *gateway*—Send the trace query to a gateway multicast address.

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

 extra-hops *extra-hops*—(Optional) Number of hops to take after reaching a nonresponsive router or switch. You can specify a number between **0** and **255**.

 group *group*—(Optional) Group address for which to trace the path. The default group address is **0.0.0.0**.

 interface *interface-name*—(Optional) Source address for sending the trace query.

 interval *interval*—(Optional) Number of seconds to wait before gathering statistics again. The default value is **10**.

 loop—(Optional) Loop indefinitely, displaying rate and loss statistics.

 max-hops *max-hops*—(Optional) Maximum hops to trace toward the source. You can specify a number between **0** and **255**. The default value is **32**.

 max-queries *max-queries*—(Optional) Maximum number of query attempts for any hop. You can specify a number between **0** and **255**. The default value is **3**.

 multicast-response—(Optional) Always request the response using multicast.

 no-resolve—(Optional) Do not attempt to display addresses symbolically.

no-router-alert—(Optional) Do not use the router-alert IP option.

response *response*—(Optional) Send trace response to a host or multicast address.

routing-instance *routing-instance-name*—(Optional) Trace a particular routing instance.

ttl *tll*—(Optional) IP time-to-live value. You can specify a number between **0** and **225**.
Local queries to the multicast group use TTL 1. Otherwise, the default value is **127**.

unicast-response—(Optional) Always request the response using unicast.

wait-time *wait-time*—(Optional) Number of seconds to wait for a response. The default value is **3**.

Required Privilege Level view

List of Sample Output [mtrace to-gateway on page 139](#)

Output Fields [Table 8 on page 139](#) describes the output fields for the **mtrace to-gateway** command. Output fields are listed in the approximate order in which they appear.

Table 8: mtrace to-gateway Output Fields

Field Name	Field Description
Mtrace from	IP address of the receiver.
to	IP address of the source.
via group	IP address of the multicast group (if any).
Querying full reverse path	Indicates the full reverse path query has begun.
number-of-hops	Number of hops from the source to the named router or switch.
router-name	Name of the router or switch for this hop.
address	Address of the router or switch for this hop.
protocol	Protocol used (for example, PIM).
Round trip time	Average round-trip time, in milliseconds (ms).
total ttl of	Time-to-live (TTL) threshold.

Sample Output

mtrace to-gateway user@host> mtrace to-gateway gateway 192.1.3.2 group 225.1.1.1 interface 192.1.1.73 brief

```
Mtrace from 192.1.1.73 to 192.1.1.2 via group 225.1.1.1
Querying full reverse path... * *
0  routerA.1ab.mycompany.net (192.1.1.2)
```

```
-1 routerA.lab.mycompany.net (192.1.1.2) PIM thresh^ 1
-2 routerB.lab.mycompany.net (192.1.2.2) PIM thresh^ 1
-3 routerC.lab.mycompany.net (192.1.3.2) PIM thresh^ 1
Round trip time 2 ms; total ttl of 3 required.
```


show igmp group

Syntax	show igmp group <brief detail> <group-name> <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	show igmp group <brief detail> <group-name>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display Internet Group Management Protocol (IGMP) group membership information.
Options	none—Display standard information about membership for all IGMP groups. brief detail—(Optional) Display the specified level of output. group-name—(Optional) Display group membership for the specified IP address only. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear igmp membership on page 114
List of Sample Output	show igmp group (Include Mode) on page 142 show igmp group (Exclude Mode) on page 143 show igmp group brief on page 143 show igmp group detail on page 143
Output Fields	Table 9 on page 141 describes the output fields for the show igmp group command. Output fields are listed in the approximate order in which they appear.

Table 9: show igmp group Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface that received the IGMP membership report. A name of local indicates that the local routing device joined the group itself.	All levels
Group	Group address.	All levels
Group Mode	Mode the SSM group is operating in: Include or Exclude .	All levels
Source	Source address.	All levels

Table 9: show igmp group Output Fields (*continued*)

Field Name	Field Description	Level of Output
Source timeout	Time remaining until the group traffic is no longer forwarded. The timer is refreshed when a listener in include mode sends a report. A group in exclude mode or configured as a static group displays a zero timer.	detail
Last reported by	Address of the host that last reported membership in this group.	All levels
Timeout	Time remaining until the group membership is removed.	brief none
Group timeout	Time remaining until a group in exclude mode moves to include mode. The timer is refreshed when a listener in exclude mode sends a report. A group in include mode or configured as a static group displays a zero timer.	detail
Type	Type of group membership: <ul style="list-style-type: none"> • Dynamic—Host reported the membership. • Static—Membership is configured. 	All levels

Sample Output

```

show igmp group (Include Mode) user@host> show igmp group
Interface: t1-0/1/0.0
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.2
    Last reported by: 10.9.5.2
    Timeout:      24 Type: Dynamic
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.3
    Last reported by: 10.9.5.2
    Timeout:      24 Type: Dynamic
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.4
    Last reported by: 10.9.5.2
    Timeout:      24 Type: Dynamic
  Group: 232.1.1.2
    Group mode: Include
    Source: 10.0.0.4
    Last reported by: 10.9.5.2
    Timeout:      24 Type: Dynamic
Interface: t1-0/1/1.0
Interface: ge-0/2/2.0
Interface: ge-0/2/0.0
Interface: local
  Group: 224.0.0.2
    Source: 0.0.0.0
    Last reported by: Local
    Timeout:      0 Type: Dynamic
  Group: 224.0.0.22
    Source: 0.0.0.0

```

```

Last reported by: Local
Timeout:          0 Type: Dynamic

```

**show igmp group
(Exclude Mode)**

```

user@host> show igmp group
Interface: t1-0/1/0.0
Interface: t1-0/1/1.0
Interface: ge-0/2/2.0
Interface: ge-0/2/0.0
Interface: local
  Group: 224.0.0.2
    Source: 0.0.0.0
    Last reported by: Local
    Timeout:          0 Type: Dynamic
  Group: 224.0.0.22
    Source: 0.0.0.0
    Last reported by: Local
    Timeout:          0 Type: Dynamic

```

show igmp group brief The output for the **show igmp group brief** command is identical to that for the **show igmp group** command.

show igmp group detail

```

user@host> show igmp group detail
Interface: t1-0/1/0.0
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.2
    Source timeout: 12
    Last reported by: 10.9.5.2
    Group timeout:          0 Type: Dynamic
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.3
    Source timeout: 12
    Last reported by: 10.9.5.2
    Group timeout:          0 Type: Dynamic
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.4
    Source timeout: 12
    Last reported by: 10.9.5.2
    Group timeout:          0 Type: Dynamic
  Group: 232.1.1.2
    Group mode: Include
    Source: 10.0.0.4
    Source timeout: 12
    Last reported by: 10.9.5.2
    Group timeout:          0 Type: Dynamic
Interface: t1-0/1/1.0
Interface: ge-0/2/2.0
Interface: ge-0/2/0.0
Interface: local
  Group: 224.0.0.2
    Group mode: Exclude
    Source: 0.0.0.0
    Source timeout: 0
    Last reported by: Local
    Group timeout:          0 Type: Dynamic
  Group: 224.0.0.22
    Group mode: Exclude
    Source: 0.0.0.0

```

Source timeout: 0
Last reported by: Local
Group timeout: 0 Type: Dynamic

show igmp interface

Syntax	show igmp interface <brief detail> <interface-name> <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	show igmp interface <brief detail> <interface-name>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display information about Internet Group Management Protocol (IGMP)-enabled interfaces.
Options	none—Display standard information about all IGMP-enabled interfaces. brief detail—(Optional) Display the specified level of output. <i>interface-name</i> —(Optional) Display information about the specified IGMP-enabled interface only. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear igmp membership on page 114
List of Sample Output	show igmp interface on page 147 show igmp interface brief on page 147 show igmp interface detail on page 147
Output Fields	Table 10 on page 145 describes the output fields for the show igmp interface command. Output fields are listed in the approximate order in which they appear.

Table 10: show igmp interface Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface.	All levels
State	State of the interface: Up or Down .	All levels
Querier	Address of the routing device that has been elected to send membership queries.	All levels
Timeout	How long until the IGMP querier is declared to be unreachable, in seconds.	All levels

Table 10: show igmp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
Version	IGMP version being used on the interface: 1, 2, or 3.	All levels
Groups	Number of groups on the interface.	All levels
Immediate Leave	State of the immediate leave option: <ul style="list-style-type: none"> • On—Indicates that the router removes a host from the multicast group as soon as the router receives a leave group message from a host associated with the interface. • Off—Indicates that after receiving a leave group message, instead of removing a host from the multicast group immediately, the router sends a group query to determine if another receiver responds. 	All levels
Promiscuous Mode	State of the promiscuous mode option: <ul style="list-style-type: none"> • On—Indicates that the router can accept IGMP reports from subnetworks that are not associated with its interfaces. • Off—Indicates that the router can accept IGMP reports only from subnetworks that are associated with its interfaces. 	All levels
Passive	State of the passive mode option: <ul style="list-style-type: none"> • On—Indicates that the router can run IGMP on the interface but not send or receive control traffic such as IGMP reports, queries, and leaves. • Off—Indicates that the router can run IGMP on the interface and send or receive control traffic such as IGMP reports, queries, and leaves. <p>The passive statement enables you to selectively activate up to two out of a possible three available query or control traffic options. When enabled, the following options appear after the on state declaration:</p> <ul style="list-style-type: none"> • send-general-query—The interface sends general queries. • send-group-query—The interface sends group-specific and group-source-specific queries. • allow-receive—The interface receives control traffic 	All levels
OIF map	Name of the OIF map associated to the interface.	All levels
SSM map	Name of the source-specific multicast (SSM) map (if configured) used on the interface.	All levels
Configured Parameters	Information configured by the user: <ul style="list-style-type: none"> • IGMP Query Interval—Interval (in seconds) at which this router sends membership queries when it is the querier. • IGMP Query Response Interval—Time (in seconds) that the router waits for a report in response to a general query. • IGMP Last Member Query Interval—Time (in seconds) that the router waits for a report in response to a group-specific query. • IGMP Robustness Count—Number of times the router retries a query. 	All levels

Table 10: show igmp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
Derived Parameters	Derived information: <ul style="list-style-type: none"> IGMP Membership Timeout—Timeout period (in seconds) for group membership. If no report is received for these groups before the timeout expires, the group membership is removed. IGMP Other Querier Present Timeout—Time (in seconds) that the router waits for the IGMP querier to send a query. 	All levels

Sample Output

show igmp interface	<pre> user@host> show igmp interface Interface: at-0/3/1.0 Querier: 10.111.30.1 State: Up Timeout: None Version: 2 Groups: 4 Interface: so-1/0/0.0 Querier: 10.111.10.1 State: Up Timeout: None Version: 2 Groups: 2 Interface: so-1/0/1.0 Querier: 10.111.20.1 State: Up Timeout: None Version: 2 Groups: 4 Immediate Leave: On Promiscuous Mode: Off Configured Parameters: IGMP Query Interval: 125.0 IGMP Query Response Interval: 10.0 IGMP Last Member Query Interval: 1.0 IGMP Robustness Count: 2 Derived Parameters: IGMP Membership Timeout: 260.0 IGMP Other Querier Present Timeout: 255.0 </pre>
show igmp interface brief	The output for the show igmp interface brief command is identical to that for the show igmp interface command. For sample output, see show igmp interface on page 147 .
show igmp interface detail	The output for the show igmp interface detail command is identical to that for the show igmp interface command. For sample output, see show igmp interface on page 147 .

show igmp statistics

Syntax	show igmp statistics <brief detail> <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	show igmp statistics <brief detail> <interface <i>interface-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display Internet Group Management Protocol (IGMP) statistics.
Options	none—Display IGMP statistics for all interfaces. brief detail—(Optional) Display the specified level of output. interface <i>interface-name</i> —(Optional) Display IGMP statistics about the specified interface only. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear igmp statistics on page 118
List of Sample Output	show igmp statistics on page 149 show igmp statistics interface on page 150
Output Fields	Table 11 on page 148 describes the output fields for the show igmp statistics command. Output fields are listed in the approximate order in which they appear.

Table 11: show igmp statistics Output Fields

Field Name	Field Description
IGMP packet statistics	Heading for IGMP packet statistics for all interfaces or for the specified interface name.

Table 11: show igmp statistics Output Fields (*continued*)

Field Name	Field Description
IGMP Message type	<p>Summary of IGMP statistics:</p> <ul style="list-style-type: none"> • Membership Query—Number of membership queries sent and received. • V1 Membership Report—Number of version 1 membership reports sent and received. • DVMRP—Number of DVMRP messages sent or received. • PIM V1—Number of PIM version 1 messages sent or received. • Cisco Trace—Number of Cisco trace messages sent or received. • V2 Membership Report—Number of version 2 membership reports sent or received. • Group Leave—Number of group leave messages sent or received. • Mtrace Response—Number of Mtrace response messages sent or received. • Mtrace Request—Number of Mtrace request messages sent or received. • Domain Wide Report—Number of domain-wide reports sent or received. • V3 Membership Report—Number of version 3 membership reports sent or received. • Other Unknown types—Number of unknown message types received. • IGMP v3 unsupported type—Number of messages received with unknown and unsupported IGMP version 3 message types. • IGMP v3 source required for SSM—Number of IGMP version 3 messages received that contained no source. • IGMP v3 mode not applicable for SSM—Number of IGMP version 3 messages received that did not contain a mode applicable for source-specific multicast (SSM).
Received	Number of messages received.
Sent	Number of messages sent.
Rx errors	Number of received packets that contained errors.
IGMP Global Statistics	<p>Summary of IGMP statistics for all interfaces.</p> <ul style="list-style-type: none"> • Bad Length—Number of messages received with length errors so severe that further classification could not occur. • Bad Checksum—Number of messages received with a bad IP checksum. No further classification was performed. • Bad Receive If—Number of messages received on an interface not enabled for IGMP. • Rx non-local—Number of messages received from senders that are not local. • Timed out—Number of groups that timed out as a result of not receiving an explicit leave message. • Rejected Report—Number of reports dropped because of the IGMP group policy. • Total Interfaces—Number of interfaces configured to support IGMP.

Sample Output

```

show igmp statistics  user@host> show igmp statistics
IGMP packet statistics for all interfaces
IGMP Message type    Received      Sent  Rx errors
Membership Query      8883         459      0
V1 Membership Report    0            0        0
DVMRP                  0            0        0
PIM V1                 0            0        0

```

Cisco Trace	0	0	0
V2 Membership Report	0	0	0
Group Leave	0	0	0
Mtrace Response	0	0	0
Mtrace Request	0	0	0
Domain Wide Report	0	0	0
V3 Membership Report	0	0	0
Other Unknown types			0
IGMP v3 unsupported type			0
IGMP v3 source required for SSM			0
IGMP v3 mode not applicable for SSM			0
IGMP Global Statistics			
Bad Length	0		
Bad Checksum	0		
Bad Receive If	0		
Rx non-local	1227		
Timed out	0		
Rejected Report	0		
Total Interfaces	2		

```
show igmp statistics interface
user@host> show igmp statistics interface fe-1/0/1.0
IGMP interface packet statistics for fe-1/0/1.0
IGMP Message type      Received      Sent  Rx errors
Membership Query        0           230      0
V1 Membership Report    0           0        0
```

show igmp-snooping membership

Syntax	show igmp-snooping membership <brief detail> <interface <i>interface-name</i> > <vlan (<i>vlan-id</i> <i>vlan-name</i>)>
Release Information	Command introduced in Junos OS Release 9.1 for EX Series switches.
Description	Display the multicast group membership information maintained by IGMP snooping.
Options	<p>none—Display the multicast group membership information for all VLANs on which IGMP snooping is enabled.</p> <p>brief detail—(Optional) Display the specified level of output. The default is brief.</p> <p>interface <i>interface-name</i>—(Optional) Display the multicast group membership information for the specified interface.</p> <p>vlan (<i>vlan-id</i> <i>vlan-name</i>)—(Optional) Display the multicast group membership for the specified VLAN.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show igmp-snooping route on page 153 • show igmp-snooping statistics on page 155 • show igmp-snooping vlans on page 157 • Monitoring IGMP Snooping on page 31 • Configuring IGMP Snooping (CLI Procedure) on page 25
List of Sample Output	show igmp-snooping membership on page 152 show igmp-snooping membership detail on page 152
Output Fields	Table 12 on page 151 lists the output fields for the show igmp-snooping membership command. Output fields are listed in the approximate order in which they appear.

Table 12: show igmp-snooping membership Output Fields

Field Name	Field Description	Level of Output
VLAN	Name of the VLAN.	All
Interfaces	Interfaces that are members of the listed multicast group.	All
Tag	Numerical identifier of the VLAN.	detail

Table 12: show igmp-snooping membership Output Fields (*continued*)

Field Name	Field Description	Level of Output
Router interfaces	<p>List of information about multicast-router interfaces:</p> <ul style="list-style-type: none"> Name of the multicast-router interface. static or dynamic—Whether the multicast router interface is static or dynamic. 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. timeout—Query timeout in seconds. 	detail
Group	<p>IP multicast address of the multicast group.</p> <p>The following information is provided for the multicast group:</p> <ul style="list-style-type: none"> Name of the interface belonging to the multicast group. timeout—Time (in seconds) left until the entry for the multicast group is removed. Last reporter—Last host to report membership for the multicast group. Receiver count—Number of interfaces that have membership in a multicast group. Flags—IGMP version of the host sending a join message. If the interface is a static group-member interface, the flag static is also included. Include source—Source addresses from which multicast streams are allowed based on IGMPv3 reports. Shown only for IGMPv3 joins. 	detail

Sample Output

```

show igmp-snooping membership user@switch> show igmp-snooping membership
                                VLAN: vlan24
                                224.1.1.1      *
                                  Interfaces: ge-0/0/0.0
                                224.1.1.100    *
                                  Interfaces: ge-0/0/0.0
                                225.1.1.100    *
                                  Interfaces: ge-0/0/0.0

show igmp-snooping membership detail user@switch> show igmp-snooping membership detail
                                VLAN: vlan24 Tag: 24 (Index: 3)
                                Router interfaces:
                                  ge-0/0/8.0 dynamic Uptime: 00:08:35 timeout: 254
                                Group: 224.1.1.1
                                  ge-0/0/0.0 timeout: 223 Receiver count: 1, Flags: <V2-hosts Static>
                                Group: 224.1.1.100
                                  ge-0/0/0.0 timeout: 170 Last reporter: 10.10.1.10 Receiver count: 1, Flags:
                                  <V2-hosts>
                                Group: 225.1.1.100
                                  ge-0/0/0.0 timeout: 168 Last reporter: 10.10.1.10 Receiver count: 1, Flags:
                                  <V2-hosts>

```

show igmp-snooping route

Syntax	<pre>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></pre>
Release Information	<p>Command introduced in Junos OS Release 9.1 for EX Series switches.</p> <p>Option inet enhanced to support IPv6 multicast groups in Junos OS Release 10.2 for EX Series switches.</p>
Description	Display IGMP snooping route information.
Options	<p>none—Display general parameters.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>ethernet-switching—(Optional) Display Ethernet switching information.</p> <p>inet—(Optional) Display inet information for IPv4 and IPv6 multicast groups. For Layer 3 IPv6 multicast routes, display information about the routing table, the routing next hop, and the Layer 2 next hop.</p> <p>vlan vlan-id vlan-name—(Optional) Display route information for the specified VLAN.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show igmp-snooping statistics on page 155 • show igmp-snooping vlans on page 157
List of Sample Output	<p>show igmp-snooping route on page 154</p> <p>show igmp-snooping route inet detail (IPv6 Multicast Route) on page 154</p> <p>show igmp-snooping route vlan v1 on page 154</p>
Output Fields	<p>Table 13 on page 153 lists the output fields for the show igmp-snooping route command. Output fields are listed in the approximate order in which they appear.</p>

Table 13: show igmp-snooping route Output Fields

Field Name	Field Description
Table	(For internal use only. Value is always 0.)
Routing Table	(For internal use only. Value is always 0.)
VLAN	Name of the VLAN on which IGMP snooping is enabled.
Group	Multicast IPv4 or IPv6 group address.

Table 13: show igmp-snooping route Output Fields (*continued*)

Field Name	Field Description
Next-hop	ID associated with the next-hop device.
Routing next-hop	ID associated with the Layer 3 next-hop device.
Interface or Interfaces	Name of the interface or interfaces in the VLAN associated with the multicast group.
Layer 2 next-hop	ID associated with the Layer 2 next-hop device.

Sample Output

```

show igmp-snooping route user@switch> 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 inet detail (IPv6 Multicast Route) user@switch> show igmp-snooping route inet detail
Routing table: 0
Group: ff0e::1:ff05:1a3d, 2001::ee0:81ff:ee05:1a2e
Routing next-hop: 587
               vlan.42
Interface: vlan.42, VLAN: v42, Layer 2 next-hop: 506

show igmp-snooping route vlan v1 user@switch> show igmp-snooping 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 OS Release 9.1 for EX Series switches.
Description	Display IGMP snooping statistics.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show igmp-snooping route on page 153 • show igmp-snooping vlans on page 157
List of Sample Output	show igmp-snooping statistics on page 155
Output Fields	Table 14 on page 155 lists the output fields for the show igmp-snooping statistics command. Output fields are listed in the approximate order in which they appear.

Table 14: 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.

Sample Output

```

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	<code>show igmp-snooping vlans</code> <code><brief detail></code> <code><vlan <i>vlan-id</i> <i>vlan-name</i>></code>
Release Information	Command introduced in Junos OS Release 9.1 for EX Series switches.
Description	Display IGMP snooping VLAN information.
Options	<p><code>none</code>—Display general parameters.</p> <p><code>brief detail</code>—(Optional) Display the specified level of output.</p> <p><code>vlan <i>vlan-id</i> vlan <i>vlan-number</i></code>—(Optional) Display VLAN information for the specified VLAN.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show igmp-snooping route on page 153 • show igmp-snooping statistics on page 155
List of Sample Output	<p>show igmp-snooping vlans on page 158</p> <p>show igmp-snooping vlans vlan v10 on page 158</p> <p>show igmp-snooping vlans vlan v10 detail on page 158</p>
Output Fields	Table 15 on page 157 lists the output fields for the show igmp-snooping vlans command. Output fields are listed in the approximate order in which they appear.

Table 15: 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 VLAN interfaces with a receiver for any group. Indicates how many VLAN interfaces would receive data because of IGMP membership.	All levels
RxVlans	Number of MVR receiver VLANs configured for that MVR source VLAN.	All levels
Tag	Numerical identifier of the VLAN.	Detail
vlan-interface	Internal VLAN interface identifier.	Detail

Table 15: show igmp-snooping vlans Output Fields (*continued*)

Field Name	Field Description	Level of Output
Membership timeout	Membership timeout value.	Detail
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

Sample Output

```

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

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

show igmp-snooping user@switch> show igmp-snooping vlans vlan v10 detail
vls 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

```

show multicast flow-map

Syntax	show multicast flow-map <brief detail> <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	show multicast flow-map <brief detail>
Release Information	Command introduced in Junos OS Release 8.2. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display configuration information about IP multicast flow maps.
Options	none—Display configuration information about IP multicast flow maps on all systems. brief detail—(Optional) Display the specified level of output. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	view
List of Sample Output	show multicast flow-map on page 160 show multicast flow-map detail on page 160
Output Fields	Table 16 on page 159 describes the output fields for the show multicast flow-map command. Output fields are listed in the approximate order in which they appear.

Table 16: show multicast flow-map Output Fields

Field Name	Field Description	Levels of Output
Name	Name of the flow map.	All levels
Policy	Name of the policy associated with the flow map.	All levels
Cache-timeout	Cache timeout value assigned to the flow map.	All levels
Bandwidth	Bandwidth setting associated to the flow map.	All levels
Adaptive	Whether or not adaptive mode is enabled for the flow map.	none
Flow-map	Name of the flow map.	detail
Adaptive Bandwidth	Whether or not adaptive mode is enabled for the flow map.	detail
Redundant Sources	Redundant sources defined for the same destination group.	detail

Sample Output

```

show multicast flow-map user@host> show multicast flow-map
Instance: master
Name          Policy          Cache timeout    Bandwidth Adaptive
map2          policy2         never            2000000 no
map1          policy1         60 seconds      2000000 no

```

Sample Output

```

show multicast flow-map detail user@host> show multicast flow-map detail
Instance: master
Flow-map: map1
Policy:          policy1
Cache Timeout:   600 seconds
Bandwidth:       2000000
Adaptive Bandwidth: yes
Redundant Sources: 11.11.11.11
Redundant Sources: 11.11.11.12
Redundant Sources: 11.11.11.13

```

show multicast interface

Syntax	show multicast interface <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	show multicast interface
Release Information	Command introduced in Junos OS Release 8.3. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display bandwidth information about IP multicast interfaces.
Options	none—Display all interfaces that have multicast configured. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	view
List of Sample Output	show multicast interface on page 162
Output Fields	Table 17 on page 161 describes the output fields for the show multicast interface command. Output fields are listed in the approximate order in which they appear.

Table 17: show multicast interface Output Fields

Field Name	Field Description
Interface	Name of the multicast interface.
Maximum bandwidth (bps)	Maximum bandwidth setting, in bits per second, for this interface.
Remaining bandwidth (bps)	Amount of bandwidth, in bits per second, remaining on the interface.
Mapped bandwidth deduction (bps)	<p>Amount of bandwidth, in bits per second, used by any flows that are mapped to the interface.</p> <p>NOTE: Adding the mapped bandwidth deduction value to the local bandwidth deduction value results in the total deduction value for the interface.</p> <p>This field does not appear in the output when the no QoS adjustment feature is disabled.</p>
Local bandwidth deduction (bps)	<p>Amount of bandwidth, in bits per second, used by any mapped flows that are traversing the interface.</p> <p>NOTE: Adding the mapped bandwidth deduction value to the local bandwidth deduction value results in the total deduction value for the interface.</p> <p>This field does not appear in the output when the no QoS adjustment feature is disabled.</p>

Table 17: show multicast interface Output Fields (*continued*)

Field Name	Field Description
Reverse OIF mapping	State of the reverse OIF mapping feature (on or off). NOTE: This field does not appear in the output when the no QoS adjustment feature is disabled.
Reverse OIF mapping no QoS adjustment	State of the no QoS adjustment feature (on or off) for interfaces that are using reverse OIF mapping. NOTE: This field does not appear in the output when the no QoS adjustment feature is disabled.
Leave timer	Amount of time a mapped interface remains active after the last mapping ends. NOTE: This field does not appear in the output when the no QoS adjustment feature is disabled.
No QoS adjustment	State (on) of the no QoS adjustment feature when this feature is enabled. NOTE: This field does not appear in the output when the no QoS adjustment feature is disabled.

Sample Output

```

show multicast interface user@host> show multicast interface
Interface                Maximum bandwidth (bps) Remaining bandwidth (bps)
fe-0/0/3                  10000000                   0
fe-0/0/3.210              10000000                  -2000000
fe-0/0/3.220             1000000000               100000000
fe-0/0/3.230              20000000                 18000000
fe-0/0/2.200             100000000               100000000

```

show multicast mrinfo

Syntax	<code>show multicast mrinfo</code> <code><host></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display configuration information about IP multicast networks, including neighboring multicast router addresses.
Options	<code>none</code> —Display configuration information about all multicast networks. <code>host</code> —(Optional) Display configuration information about a particular host. Replace <code>host</code> with a hostname or IP address.
Required Privilege Level	view
List of Sample Output	show multicast mrinfo on page 164
Output Fields	Table 18 on page 163 describes the output fields for the show multicast mrinfo command. Output fields are listed in the approximate order in which they appear.

Table 18: show multicast mrinfo Output Fields

Field Name	Field Description
<i>source-address</i>	Query address, hostname (DNS name or IP address of the source address), and multicast protocol version or the software version of another vendor.
<i>ip-address-1—>ip-address-2</i>	Queried router interface address and directly attached neighbor interface address, respectively.
<i>(name or ip-address)</i>	Name or IP address of neighbor.
<i>[metric/threshold/type/flags]</i>	Neighbor's multicast profile: <ul style="list-style-type: none"> metric—Always has a value of 1, because mrinfo queries the directly connected interfaces of a device. threshold—Multicast threshold time-to-live (TTL). The range of values is 0 through 255. type—Multicast connection type: pim or tunnel. flags—Flags for this route: <ul style="list-style-type: none"> querier—Queried router is the designated router for the neighboring session. leaf—Link is a leaf in the multicast network. down—Link status indicator.

Sample Output

```
show multicast mrinfo  user@host> show multicast mrinfo 10.35.4.1
10.35.4.1 (10.35.4.1) [version 12.0]:
  192.168.195.166 -> 0.0.0.0 (local) [1/0/pim/querier/leaf]
  10.38.20.1 -> 0.0.0.0 (local) [1/0/pim/querier/leaf]
  10.47.1.1 -> 10.47.1.2 (10.47.1.2) [1/5/pim]
  0.0.0.0 -> 0.0.0.0 (local) [1/0/pim/down]
```


show multicast next-hops

Syntax	<pre>show multicast next-hops <brief detail> <identifier-number> <inet inet6> <logical-system (all <i>logical-system-name</i>)></pre>
Syntax (EX Series Switch)	<pre>show multicast next-hops <brief detail> <identifier-number> <inet inet6></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>inet6 option introduced in Junos OS Release 10.0 for EX Series switches.</p> <p>detail option display of next-hop ID number introduced in Junos OS Release 11.1 for M series and T series routers and EX Series switches.</p>
Description	Display the entries in the IP multicast next-hop table.
Options	<p>none—Display standard information about all entries in the multicast next-hop table for all supported address families.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>When you include the detail option on M Series and T Series routers and EX Series switches, the downstream interface name includes the next-hop ID number in parentheses, in the form fe-0/1/2.0-(1048574) where 1048574 is the next-hop ID number.</p> <p>identifier-number—(Optional) Show a particular next hop by ID number. The range of values is 1 through 65,535.</p> <p>inet inet6—(Optional) Display entries for IPv4 or IPv6 family addresses, respectively.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Required Privilege Level	view
List of Sample Output	<p>show multicast next-hops on page 166</p> <p>show multicast next-hops brief on page 166</p> <p>show multicast next-hops detail on page 166</p>
Output Fields	<p>Table 19 on page 166 describes the output fields for the show multicast next-hops command. Output fields are listed in the approximate order in which they appear.</p>

Table 19: show multicast next-hops Output Fields

Field Name	Field Description
ID	Next-hop identifier of the prefix. The identifier is returned by the routing device's Packet Forwarding Engine.
Refcnt	Number of cache entries that are using this next hop.
KRefCount	Kernel reference count for the next hop.
Downstream interface	Interface names associated with each multicast next-hop ID.

Sample Output

```

user@host> show multicast next-hops
Family: INET
ID      Refcount  KRefCount  Downstream interface
262142      4          2  so-1/0/0.0
262143      2          1  mt-1/1/0.49152
262148      2          1  mt-1/1/0.32769

Family: INET6

```

The output for the **show multicast next-hops brief** command is identical to that for the **show multicast next-hops** command. For sample output, see [show multicast next-hops on page 166](#).

```

user@host> show multicast next-hops detail
Family: INET
ID      Refcount  KRefCount  Downstream interface
1048577      2          1  fe-0/1/2.0-(1048574)
                                ge-0/2/3.0-(1048576)

```

show multicast pim-to-igmp-proxy

Syntax	show multicast pim-to-igmp-proxy <instance <i>instance-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	show multicast pim-to-igmp-proxy <instance <i>instance-name</i> >
Release Information	Command introduced in Junos OS Release 9.6. Command introduced in Junos OS Release 9.6 for EX Series switches. instance option introduced in Junos OS Release 10.0. instance option introduced in Junos OS Release 10.0 for EX Series switches.
Description	Display configuration information about PIM-to-IGMP message translation, also known as PIM-to-IGMP proxy.
Options	none—Display configuration information about PIM-to-IGMP message translation for all routing instances. instance <i>instance-name</i> —(Optional) Display configuration information about PIM-to-IGMP message translation for a specific multicast instance. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	view
List of Sample Output	show multicast pim-to-igmp-proxy on page 167 show multicast pim-to-igmp-proxy instance on page 168
Output Fields	Table 20 on page 167 describes the output fields for the show multicast pim-to-igmp-proxy command. Output fields are listed in the order in which they appear.

Table 20: show multicast pim-to-igmp-proxy Output Fields

Field Name	Field Description
Proxy state	State of PIM-to-IGMP message translation, also known as PIM-to-IGMP proxy, on the configured upstream interfaces: enabled or disabled .
<i>interface-name</i>	Name of upstream interface (no more than two allowed) on which PIM-to-IGMP message translation is configured.

Sample Output

```

show multicast pim-to-igmp-proxy
user@host> show multicast pim-to-igmp-proxy
Instance: master Proxy state: enabled
ge-0/1/0.1
ge-0/1/0.2

```

show multicast	user@host> show multicast pim-to-igmp-proxy instance VPN-A
pim-to-igmp-proxy	Instance: VPN-A Proxy state: enabled
instance	ge-0/1/0.1

show multicast pim-to-mld-proxy

Syntax	show multicast pim-to-mld-proxy <instance <i>instance-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	show multicast pim-to-mld-proxy <instance <i>instance-name</i> >
Release Information	Command introduced in Junos OS Release 9.6. Command introduced in Junos OS Release 9.6 for EX Series switches. instance option introduced in Junos OS Release 10.0. instance option introduced in Junos OS Release 10.0 for EX Series switches.
Description	Display configuration information about PIM-to-MLD message translation, also known as PIM-to-MLD proxy.
Options	none—Display configuration information about PIM-to-MLD message translation for all routing instances. instance <i>instance-name</i> —(Optional) Display configuration information about PIM-to-MLD message translation for a specific multicast instance. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	view
List of Sample Output	show multicast pim-to-mld-proxy on page 169 show multicast pim-to-mld-proxy instance on page 170
Output Fields	Table 21 on page 169 describes the output fields for the show multicast pim-to-mld-proxy command. Output fields are listed in the order in which they appear.

Table 21: show multicast pim-to-mld-proxy Output Fields

Field Name	Field Description
Proxy state	State of PIM-to-MLD message translation, also known as PIM-to-MLD proxy, on the configured upstream interfaces: enabled or disabled .
<i>interface-name</i>	Name of upstream interface (no more than two allowed) on which PIM-to-MLD message translation is configured.

Sample Output

```

show multicast pim-to-mld-proxy user@host> show multicast pim-to-mld-proxy
Instance: master Proxy state: enabled
ge-0/5/0.1
ge-0/5/0.2

```

```
show multicast      user@host> show multicast pim-to-mld-proxy instance VPN-A
pim-to-mld-proxy    Instance: VPN-A Proxy state: enabled
instance            ge-0/5/0.1
```

show multicast route

Syntax	<pre>show multicast route <brief detail extensive> <active all inactive> <group group> <inet inet6> <instance instance name> <logical-system (all logical-system-name)> <regular-expression> <source-prefix source-prefix></pre>
Syntax (EX Series Switch)	<pre>show multicast route <brief detail extensive> <active all inactive> <group group> <inet inet6> <instance instance name> <regular-expression> <source-prefix source-prefix></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.</p>
Description	<p>Display the entries in the IP multicast forwarding table. You can display similar information with the show route table inet.1 command.</p>
Options	<p>none—Display standard information about all entries in the multicast forwarding table for all routing instances.</p> <p>brief detail extensive—(Optional) Display the specified level of output.</p> <p>active all inactive—(Optional) Display all active entries, all entries, or all inactive entries, respectively, in the multicast forwarding table.</p> <p>group group—(Optional) Display the cache entries for a particular group.</p> <p>inet inet6—(Optional) Display multicast forwarding table entries for IPv4 or IPv6 family addresses, respectively.</p> <p>instance instance-name—(Optional) Display entries in the multicast forwarding table for a specific multicast instance.</p> <p>logical-system (all logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> <p>regular-expression—(Optional) Display information about the multicast forwarding table entries that match a UNIX-style regular expression.</p> <p>source-prefix source-prefix—(Optional) Display the cache entries for a particular source prefix.</p>

Required Privilege Level view

List of Sample Output [show multicast route on page 173](#)
[show multicast route brief on page 173](#)
[show multicast route detail on page 173](#)
[show multicast route extensive on page 174](#)
[show multicast route instance <instance-name> extensive on page 175](#)

Output Fields Table 22 on page 172 describes the output fields for the **show multicast route** command. Output fields are listed in the approximate order in which they appear.

Table 22: show multicast route Output Fields

Field Name	Field Description	Level of Output
Address family	IPv4 address family (INET) or IPv6 address family (INET6).	All levels
Group	Group address.	All levels
Source	Prefix and length of the source as it is in the multicast forwarding table.	All levels
Upstream interface	Name of the interface on which the packet with this source prefix is expected to arrive.	All levels
Downstream interface list	List of interface names to which the packet with this source prefix is forwarded.	All levels
Session description	Name of the multicast session.	detail extensive
Statistics	Rate at which packets are being forwarded for this source and group entry (in Kbps and pps), and number of packets that have been forwarded to this prefix. If one or more of the kilobits per second packet forwarding statistic queries fails or times out, the statistics field displays Forwarding statistics are not available .	detail extensive
Next-hop ID	Next-hop identifier of the prefix. The identifier is returned by the routing device's Packet Forwarding Engine and is also displayed in the output of the show multicast nexthops command.	detail extensive
Upstream protocol	Protocol running on the interface on which the packet with this source prefix is expected to arrive.	detail extensive
Route state	Whether the group is Active or Inactive .	extensive
Forwarding state	Whether the prefix is pruned or forwarding.	extensive
Cache lifetime/timeout	Number of seconds until the prefix is removed from the multicast forwarding table. A value of never indicates a permanent forwarding entry.	extensive
Wrong incoming interface notifications	Number of times that the upstream interface was not available.	extensive

Sample Output

```

show multicast route user@host> show multicast route
Family: INET

Group: 228.0.0.0
Source: 10.255.14.144/32
Upstream interface: local
Downstream interface list:
    so-1/0/0.0

Group: 239.1.1.1
Source: 10.255.14.144/32
Upstream interface: local
Downstream interface list:
    so-1/0/0.0

Group: 239.1.1.1
Source: 10.255.70.15/32
Upstream interface: so-1/0/0.0
Downstream interface list:
    mt-1/1/0.49152

Family: INET6

show multicast route brief The output for the show multicast route brief command is identical to that for the show
multicast route command. For sample output, see show multicast route on page 173.

show multicast route detail user@host> show multicast route detail
Family: INET

Group: 228.0.0.0
Source: 10.255.14.144/32
Upstream interface: local
Downstream interface list:
    so-1/0/0.0
Session description: Unknown
Statistics: 8 kbps, 100 pps, 45272 packets
Next-hop ID: 262142
Upstream protocol: PIM

Group: 239.1.1.1
Source: 10.255.14.144/32
Upstream interface: local
Downstream interface list:
    so-1/0/0.0
Session description: Administratively Scoped
Statistics: 0 kbps, 0 pps, 13404 packets
Next-hop ID: 262142
Upstream protocol: PIM

Group: 239.1.1.1
Source: 10.255.70.15/32
Upstream interface: so-1/0/0.0
Downstream interface list:
    mt-1/1/0.49152
Session description: Administratively Scoped
Statistics: 46 kbps, 1000 pps, 921077 packets

```

Next-hop ID: 262143
Upstream protocol: PIM

Family: INET6

**show multicast route
extensive**

```
user@host> show interfaces mt-2/1/10 extensive
Physical interface: mt-2/1/10, Enabled, Physical link is Up
Interface index: 262, SNMP ifIndex: 677, Generation: 265
Type: Multicast-GRE, Link-level type: GRE, MTU: Unlimited, Speed: 1000mbps
Hold-times      : Up 0 ms, Down 0 ms
Device flags    : Present Running
Interface flags: SNMP-Traps
Statistics last cleared: Never
Traffic statistics:
  Input bytes   :           5238           0 bps
  Output bytes  :        31117424       416120 bps
  Input packets :           97           0 pps
  Output packets:        598412       1000 pps
IPv6 transit statistics:
  Input bytes   :           0
  Output bytes  :           0
  Input packets :           0
  Output packets:           0

Logical interface mt-2/1/10.32768 (Index 88) (SNMP ifIndex 680) (Generation
165)
Flags: Point-To-Point SNMP-Traps 0x4000 IP-Header
232.1.1.1:10.0.0.17:47:df:64:0000000800000000 Encapsulation: GRE-NULL
Traffic statistics:
  Input bytes   :           0
  Output bytes  :        31119218
  Input packets :           0
  Output packets:        598435
IPv6 transit statistics:
  Input bytes   :           0
  Output bytes  :           0
  Input packets :           0
  Output packets:           0
Local statistics:
  Input bytes   :           0
  Output bytes  :         1794
  Input packets :           0
  Output packets:          23
Transit statistics:
  Input bytes   :           0           0 bps
  Output bytes  :        31117424       416120 bps
  Input packets :           0           0 pps
  Output packets:        598412       1000 pps
IPv6 transit statistics:
  Input bytes   :           0
  Output bytes  :           0
  Input packets :           0
  Output packets:           0
Protocol inet, MTU: 4446, Generation: 200, Route table: 4
Flags: None
Protocol inet6, MTU: 4446, Generation: 201, Route table: 4
Flags: None

Logical interface mt-2/1/10.1081344 (Index 89) (SNMP ifIndex 681) (Generation
166)
Flags: Point-To-Point SNMP-Traps 0x6000 Encapsulation: GRE-NULL
```

```

Traffic statistics:
Input bytes :          5238
Output bytes :          0
Input packets:         97
Output packets:        0
IPv6 transit statistics:
Input bytes :          0
Output bytes :          0
Input packets:         0
Output packets:        0
Local statistics:
Input bytes :          5238
Output bytes :          0
Input packets:         97
Output packets:        0
Transit statistics:
Input bytes :          0          0 bps
Output bytes :          0          0 bps
Input packets:         0          0 pps
Output packets:        0          0 pps
IPv6 transit statistics:
Input bytes :          0
Output bytes :          0
Input packets:         0
Output packets:        0
Protocol inet, MTU: Unlimited, Generation: 202, Route table: 4
Flags: None
Protocol inet6, MTU: Unlimited, Generation: 203, Route table: 4
Flags: None

```

```

show multicast route instance mvpn extensive
instance
<instance-name>
extensive
user@host>show multicast route instance mvpn extensive
Family: INET
Group: 239.10.10.10
Source: 2.0.0.2/32
Upstream interface: xe-0/0/0.102
Downstream interface list:
    xe-10/3/0.0 xe-0/3/0.0 xe-0/0/0.106 xe-0/0/0.105
    xe-0/0/0.103 xe-0/0/0.104 xe-0/0/0.107 xe-0/0/0.108
Session description: Administratively Scoped
Statistics: 256 kbps, 3998 pps, 670150 packets
Next-hop ID: 1048579
Upstream protocol: MVPN
Route state: Active
Forwarding state: Forwarding
Cache lifetime/timeout: forever
Wrong incoming interface notifications: 58

```

show multicast rpf

Syntax	show multicast rpf <inet inet6> <instance <i>instance-name</i> > <logical-system (all <i>logical-system-name</i>)> <prefix> <summary>
Syntax (EX Series Switch)	show multicast rpf <inet inet6> <instance <i>instance-name</i> > <prefix> <summary>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Description	Display information about multicast reverse-path-forwarding (RPF) calculations.
Options	none—Display RPF calculation information for all supported address families. inet inet6—(Optional) Display the RPF calculation information for IPv4 or IPv6 family addresses, respectively. instance <i>instance-name</i> —(Optional) Display information about multicast RPF calculations for a specific multicast instance. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system. prefix—(Optional) Display the RPF calculation information for the specified prefix. summary—(Optional) Display summary of all multicast RPF information.
Required Privilege Level	view
List of Sample Output	show multicast rpf on page 177 show multicast rpf inet6 on page 178 show multicast rpf prefix on page 179 show multicast rpf summary on page 179

Output Fields Table 23 on page 177 describes the output fields for the **show multicast rpf** command. Output fields are listed in the approximate order in which they appear.

Table 23: show multicast rpf Output Fields

Field Name	Field Description
Instance	Name of the routing instance. (Displayed when multicast is configured within a routing instance.)
Source prefix	Prefix and length of the source as it exists in the multicast forwarding table.
Protocol	How the route was learned.
Interface	Upstream RPF interface.
Neighbor	Upstream RPF neighbor.

Sample Output

```

show multicast rpf user@host> show multicast rpf

Multicast RPF table: inet.0, 12 entries

0.0.0.0/0
  Protocol: Static

10.255.14.132/32
  Protocol: Direct
  Interface: lo0.0

10.255.245.91/32
  Protocol: IS-IS
  Interface: so-1/1/1.0
  Neighbor: 192.168.195.21

127.0.0.1/32
Inactive172.16.0.0/12
Protocol: Static
Interface: fxp0.0
Neighbor: 192.168.14.254

192.168.0.0/16
Protocol: Static
Interface: fxp0.0
Neighbor: 192.168.14.254

192.168.14.0/24
Protocol: Direct
Interface: fxp0.0

192.168.14.132/32
Protocol: Local

192.168.195.20/30
Protocol: Direct

```

```
Interface: so-1/1/1.0
192.168.195.22/32
Protocol: Local

192.168.195.36/30
Protocol: IS-IS
Interface: so-1/1/1.0
Neighbor: 192.168.195.21
```

```
show multicast rpf inet6 user@host> show multicast rpf inet6
inet6 Multicast RPF table: inet6.0, 12 entries

::10.255.14.132/128
    Protocol: Direct
    Interface: lo0.0

::10.255.245.91/128
    Protocol: IS-IS
    Interface: so-1/1/1.0
    Neighbor: fe80::2a0:a5ff:fe28:2e8c

::192.168.195.20/126
    Protocol: Direct
    Interface: so-1/1/1.0

::192.168.195.22/128
    Protocol: Local

::192.168.195.36/126
    Protocol: IS-IS
    Interface: so-1/1/1.0
    Neighbor: fe80::2a0:a5ff:fe28:2e8c

::192.168.195.76/126
    Protocol: Direct
    Interface: fe-2/2/0.0

::192.168.195.77/128
    Protocol: Local

fe80::/64
    Protocol: Direct
    Interface: so-1/1/1.0

fe80::290:69ff:fe0c:993a/128
    Protocol: Local

fe80::2a0:a5ff:fe12:84f/128
    Protocol: Direct
    Interface: lo0.0

ff02::2/128
    Protocol: PIM

ff02::d/128
```

Protocol: PIM

```
show multicast rpf prefix user@host> show multicast rpf ff02::/16
Multicast RPF table: inet6.0, 13 entries
ff02::2/128
    Protocol: PIM
ff02::d/128
    Protocol: PIM
...
```

```
show multicast rpf summary user@host> show multicast rpf summary
Multicast RPF table: inet.0, 16 entries
Multicast RPF table: inet6.0, 12 entries
```

show multicast scope

Syntax	show multicast scope <inet inet6> <instance <i>instance-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	show multicast scope <inet inet6> <instance <i>instance-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Description	Display administratively scoped IP multicast information.
Options	<p>none—Display standard information about administratively scoped multicast information for all supported address families in all routing instances.</p> <p>inet inet6—(Optional) Display scoped multicast information for IPv4 or IPv6 family addresses, respectively.</p> <p>instance <i>instance-name</i>—(Optional) Display administratively scoped information for a specific multicast instance.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Required Privilege Level	view
List of Sample Output	show multicast scope on page 181 show multicast scope inet on page 181 show multicast scope inet6 on page 181
Output Fields	Table 24 on page 180 describes the output fields for the show multicast scope command. Output fields are listed in the approximate order in which they appear.

Table 24: show multicast scope Output Fields

Field Name	Field Description
Scope name	Name of the multicast scope.
Group Prefix	Range of multicast groups that are scoped.
Interface	Interface that is the boundary of the administrative scope.
Resolve Rejects	Number of kernel resolve rejects.

Sample Output

```

show multicast scope user@host> show multicast scope

Scope name      Group Prefix      Interface      Resolve
Rejects
232-net         232.232.0.0/16    fe-0/0/0.1     0
local          239.255.0.0/16    fe-0/0/0.1     0
local          ff05::/16         fe-0/0/0.1     0
larry          ff05::1234/128    fe-0/0/0.1     0

```

```

show multicast scope user@host> show multicast scope inet

Scope name      Group Prefix      Interface      Resolve
Rejects
232-net         232.232.0.0/16    fe-0/0/0.1     0
local          239.255.0.0/16    fe-0/0/0.1     0

```

```

show multicast scope user@host> show multicast scope inet6

Scope name      Group Prefix      Interface      Resolve
Rejects
local          ff05::/16         fe-0/0/0.1     0
larry          ff05::1234/128    fe-0/0/0.1     0

```

show multicast sessions

Syntax	show multicast sessions <brief detail extensive> <logical-system (all <i>logical-system-name</i>)> < <i>regular-expression</i> >
Syntax (EX Series Switch)	show multicast sessions <brief detail extensive> < <i>regular-expression</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display information about announced IP multicast sessions.
Options	none—Display standard information about all multicast sessions for all routing instances. brief detail extensive—(Optional) Display the specified level of output. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system. <i>regular-expression</i> —(Optional) Display information about announced sessions that match a UNIX-style regular expression.
Required Privilege Level	view
List of Sample Output	show multicast sessions on page 183 show multicast sessions regular-expression detail on page 183
Output Fields	Table 25 on page 182 describes the output fields for the show multicast sessions command. Output fields are listed in the approximate order in which they appear.

Table 25: show multicast sessions Output Fields

Field Name	Field Description
<i>session-name</i>	Name of the known announced multicast sessions.

Sample Output

```

show multicast sessions user@host> show multicast sessions
1-Department of Biological Sciences, LSU
...
Monterey Bay - DockCam
Monterey Bay - JettyCam
Monterey Bay - StandCam
Monterey DockCam
Monterey DockCam / ROV cam
...
NASA TV (MPEG-1)
...
UO Broadcast - NASA Videos - 25 Years of Progress
UO Broadcast - NASA Videos - Journey through the Solar System
UO Broadcast - NASA Videos - Life in the Universe
UO Broadcast - NASA Videos - Nasa and the Airplane
UO Broadcasts OPB's Oregon Story
UO DOD News Clips
UO Medical Management of Biological Casualties (1)
UO Medical Management of Biological Casualties (2)
UO Medical Management of Biological Casualties (3)
...
376 active sessions.

show multicast sessions "NASA TV" detail user@host> show multicast sessions "NASA TV" detail
regular-expression sessions SDP Version: 0 Originated by: -@128.223.83.33
detail Session: NASA TV (MPEG-1)
Description: NASA television in MPEG-1 format, provided by Private University.
Please contact the UO if you have problems with this feed.
Email: Your Name Here <multicast@lists.private.edu>
Phone: Your Name Here <888/555-1212>
Bandwidth: AS:1000
Start time: permanent
Stop time: none
Attribute: type:broadcast
Attribute: tool:IP/TV Content Manager 3.4.14
Attribute: live:capture:1
Attribute: x-iptv-capture:mp1s
Media: video 54302 RTP/AVP 32 31 96 97
Connection Data: 224.2.231.45 ttl 127
Attribute: quality:8
Attribute: framerate:30
Attribute: rtpmap:96 WBIH/90000
Attribute: rtpmap:97 MP4V-ES/90000
Attribute: x-iptv-svr:video 128.223.91.191 live
Attribute: fntp:32 type=mpeg1
Media: audio 28848 RTP/AVP 14 0 96 3 5 97 98 99 100 101 102 10 11 103 104 105 106
Connection Data: 224.2.145.37 ttl 127
Attribute: rtpmap:96 X-WAVE/8000
Attribute: rtpmap:97 L8/8000/2
Attribute: rtpmap:98 L8/8000
Attribute: rtpmap:99 L8/22050/2
Attribute: rtpmap:100 L8/22050
Attribute: rtpmap:101 L8/11025/2
Attribute: rtpmap:102 L8/11025
Attribute: rtpmap:103 L16/22050/2
Attribute: rtpmap:104 L16/22050

```

1 matching sessions.

show multicast usage

Syntax	show multicast usage <brief detail> <inet inet6> <instance <i>instance-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	show multicast usage <brief detail> <inet inet6> <instance <i>instance-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Description	Display usage information about the 10 most active Distance Vector Multicast Routing Protocol (DVMRP) or Protocol Independent Multicast (PIM) groups.
Options	<p>none—Display multicast usage information for all supported address families for all routing instances.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>inet inet6—(Optional) Display usage information for IPv4 or IPv6 family addresses, respectively.</p> <p>instance <i>instance-name</i>—(Optional) Display information about the most active DVMRP or PIM groups for a specific multicast instance.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Required Privilege Level	view
List of Sample Output	show multicast usage on page 186 show multicast usage brief on page 186 show multicast usage instance on page 186 show multicast usage detail on page 186
Output Fields	Table 26 on page 185 describes the output fields for the show multicast usage command. Output fields are listed in the approximate order in which they appear.

Table 26: show multicast usage Output Fields

Field Name	Field Description
Instance	Name of the routing instance. (Displayed when multicast is configured within a routing instance.)

Table 26: show multicast usage Output Fields (*continued*)

Field Name	Field Description
Group	Group address.
Sources	Number of sources.
Packets	Number of packets that have been forwarded to this prefix. If one or more of the packets forwarded statistic queries fails or times out, the packets field displays unavailable .
Bytes	Number of bytes that have been forwarded to this prefix. If one or more of the packets forwarded statistic queries fails or times out, the bytes field displays unavailable .
Prefix	IP address.
/len	Prefix length.
Groups	Number of multicast groups.

Sample Output

```

user@host> show multicast usage
Group          Sources  Packets      Bytes
228.0.0.0      1        52847        4439148
239.1.1.1      2        13450        1125530

Prefix         /len  Groups  Packets      Bytes
10.255.14.144  /32   2        66254        5561304
10.255.70.15   /32   1         43          3374...
```

show multicast usage brief The output for the **show multicast usage brief** command is identical to that for the **show multicast usage** command. For sample output, see [show multicast usage on page 186](#).

```

user@host> show multicast usage instance VPN-A
Group          Sources  Packets      Bytes
224.2.127.254  1        5538         509496
224.0.1.39     1         13           624
224.0.1.40     1         13           624

Prefix         /len  Groups  Packets      Bytes
192.168.195.34 /32   1        5538         509496
10.255.14.30   /32   1         13           624
10.255.245.91  /32   1         13           624
...
```

```

user@host> show multicast usage detail
Group          Sources  Packets      Bytes
228.0.0.0      1        53159        4465356
  Source: 10.255.14.144 /32 Packets: 53159 Bytes: 4465356
239.1.1.1      2        13450        1125530
  Source: 10.255.14.144 /32 Packets: 13407 Bytes: 1122156
```

Source: 10.255.70.15 /32 Packets: 43 Bytes: 3374

Prefix	/len	Groups	Packets	Bytes
10.255.14.144	/32	2	66566	5587512
Group: 228.0.0.0			Packets: 53159	Bytes: 4465356
Group: 239.1.1.1			Packets: 13407	Bytes: 1122156
10.255.70.15	/32	1	43	3374
Group: 239.1.1.1			Packets: 43	Bytes: 3374

show pim bootstrap

Syntax	show pim bootstrap <instance <i>instance-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	show pim bootstrap <instance <i>instance-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. instance option introduced in Junos OS Release 10.0 for EX Series switches.
Description	For sparse mode only, display information about Protocol Independent Multicast (PIM) bootstrap routers.
Options	none—Display PIM bootstrap router information for all routing instances. instance <i>instance-name</i> —(Optional) Display information about bootstrap routers for a specific PIM-enabled routing instance. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	view
List of Sample Output	show pim bootstrap on page 189 show pim bootstrap instance on page 189
Output Fields	Table 27 on page 188 describes the output fields for the show pim bootstrap command. Output fields are listed in the approximate order in which they appear.

Table 27: show pim bootstrap Output Fields

Field Name	Field Description
Instance	Name of the routing instance.
BSR	Bootstrap router.
Pri	Priority of the routing device to be elected to be the bootstrap router.
Local address	Local routing device's address.
Pri	Local routing device's address priority to be elected as the bootstrap router.
State	Local routing device's election state: Candidate , Elected , or Ineligible .
Timeout	How long until the local routing device declares the bootstrap router to be unreachable, in seconds.

Sample Output

```

show pim bootstrap user@host> show pim bootstrap
Instance: PIM.master

BSR                Pri Local address      Pri State      Timeout
None                0 10.255.71.46      0 InEligible    0
feco:1:1:1:1:0:aff:785c 34 feco:1:1:1:1:0:aff:7c12 0 InEligible    0

```



```

show pim bootstrap user@host> show pim bootstrap instance VPN-A
instance           Instance: PIM.VPN-A

BSR                Pri Local address  Pri State      Timeout
None                0 192.168.196.105   0 InEligible    0

```

show pim interfaces

Syntax	show pim interfaces <inet inet6> <instance <i>instance-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	show pim interfaces <inet inet6> <instance <i>instance-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Description	Display information about the interfaces on which Protocol Independent Multicast (PIM) is configured.
Options	<p>none—Display interface information for all family addresses for all routing instances.</p> <p>inet inet6—(Optional) Display interface information for IPv4 or IPv6 family addresses, respectively.</p> <p>instance <i>instance-name</i>—(Optional) Display information about interfaces for a specific PIM-enabled routing instance.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Required Privilege Level	view
List of Sample Output	show pim interfaces on page 191 show pim interfaces inet on page 192 show pim interfaces inet6 on page 192
Output Fields	Table 28 on page 190 describes the output fields for the show pim interfaces command. Output fields are listed in the approximate order in which they appear.

Table 28: show pim interfaces Output Fields

Field Name	Field Description
Instance	Name of the routing instance.
Name	Interface name.
State	State of the interface. The state also is displayed in the show interfaces command.

Table 28: show pim interfaces Output Fields (*continued*)

Field Name	Field Description
Mode	<p>PIM mode running on the interface:</p> <ul style="list-style-type: none"> • Sparse—In sparse mode, routing devices must join and leave multicast groups explicitly. Upstream routing devices do not forward multicast traffic to this routing device unless this device has sent an explicit request (using a join message) to receive multicast traffic. • Dense—Unlike sparse mode, where data is forwarded only to routing devices sending an explicit request, dense mode implements a flood-and-prune mechanism, similar to DVMRP (the first multicast protocol used to support the multicast backbone). • Sparse-Dense—Sparse-dense mode allows the interface to operate on a per-group basis in either sparse or dense mode. A group specified as dense is not mapped to a rendezvous point (RP). Instead, data packets destined for that group are forwarded using PIM-Dense Mode (PIM-DM) rules. A group specified as sparse is mapped to an RP, and data packets are forwarded using PIM-Sparse Mode (PIM-SM) rules.
IP	Version number of the address family on the interface: 4 (IPv4) or 6 (IPv6).
V	PIM version running on the interface: 1 or 2.
State	<p>State of PIM on the interface:</p> <ul style="list-style-type: none"> • DR—Designated router. • NotDR—Not the designated router. • P2P—Point to point.
NbrCnt	Number of neighbors that have been seen on the interface.
JoinCnt(sg)	Number of (s,g) join messages that have been seen on the interface.
JointCnt(*g)	Number of (*g) join messages that have been seen on the interface.
DR address	Address of the designated router.

Sample Output

```

show pim interfaces  user@host> show pim interfaces
Instance: PIM.master

Name          Stat Mode   IP V State NbrCnt JoinCnt(sg) JointCnt(*g) DR
address
fe-0/0/0.0    Up   Sparse   4 2 DR      1         1           3
10.10.10.2
fe-0/0/3.0    Up   Sparse   4 2 DR      1         1           3
20.20.20.2
lo0.0         Up   Sparse   4 2 DR      0         0           0
10.255.72.54
pe-1/2/0.32769 Up   Sparse   4 2 P2P     0         0           0
t1-0/1/0.0    Up   Sparse   4 2 P2P     1         0           0
lo0.0         Up   Sparse   6 2 DR      0         0           0
fe80::2a0:a5ff:fe5e:209

```

```
show pim interfaces user@host> show pim interfaces inet
inet Instance: PIM.master
```

Name address	Stat	Mode	IP V State	NbrCnt	JoinCnt(sg)	JointCnt(*g)	DR
fe-0/0/0.0 10.10.10.2	Up	Sparse	4 2 DR	1	1	3	
fe-0/0/3.0 20.20.20.2	Up	Sparse	4 2 DR	1	1	3	
lo0.0 10.255.72.54	Up	Sparse	4 2 DR	0	0	0	
pe-1/2/0.32769	Up	Sparse	4 2 P2P	0	0	0	
tl-0/1/0.0	Up	Sparse	4 2 P2P	1	0	0	

```
show pim interfaces user@host> show pim interfaces inet6
inet6 Instance: PIM.master
```

Name address	Stat	Mode	IP V State	NbrCnt	JoinCnt(sg)	JointCnt(*g)	DR
lo0.0 fe80::2a0:a5ff:fe5e:209	Up	Sparse	6 2 DR	0	0	0	

show pim join

Syntax	<pre>show pim join <brief detail extensive summary> <inet inet6> <instance <i>instance-name</i>> <logical-system (all <i>logical-system-name</i>)> <range></pre>
Syntax (EX Series Switch)	<pre>show pim join <brief detail extensive summary> <inet inet6> <instance <i>instance-name</i>> <range></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>summary option introduced in Junos OS Release 9.6.</p> <p>inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.</p>
Description	Display information about Protocol Independent Multicast (PIM) groups.
Options	<p>none—Display the standard information about PIM groups for all supported family addresses for all routing instances.</p> <p>brief detail extensive summary—(Optional) Display the specified level of output.</p> <p>inet inet6—(Optional) Display PIM group information for IPv4 or IPv6 family addresses, respectively.</p> <p>instance <i>instance-name</i>—(Optional) Display information about groups for the specified PIM-enabled routing instance only.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> <p>range—(Optional) Address range of the group, specified as <i>prefix/prefix-length</i>.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear pim join on page 127
List of Sample Output	<p>show pim join summary on page 195</p> <p>show pim join on page 195</p> <p>show pim join instance on page 196</p> <p>show pim join detail on page 196</p> <p>show pim join extensive on page 197</p> <p>show pim join instance extensive on page 197</p>

Output Fields Table 29 on page 194 describes the output fields for the **show pim join** command. Output fields are listed in the approximate order in which they appear.

Table 29: show pim join Output Fields

Field Name	Field Description	Level of Output
Instance	Name of the routing instance.	brief detail extensive summary none
Family	Name of the address family: inet (IPv4) or inet6 (IPv6).	brief detail extensive summary none
Route type	Type of multicast route: (S,G) or (*,G).	summary
Route count	Number of (S,G) routes and number of (*,G) routes.	summary
R	Rendezvous Point Tree	brief detail extensive none
S	Sparse	brief detail extensive none
W	Wildcard	brief detail extensive none
Group	Group address.	brief detail extensive none
Source	Multicast source: <ul style="list-style-type: none"> • * (wildcard value) • <i>ipv4-address</i> • <i>ipv6-address</i> 	brief detail extensive none
RP	Rendezvous point for the PIM group.	brief detail extensive none
Flags	PIM flags: <ul style="list-style-type: none"> • dense—Dense mode entry. • rptree—Entry is on the rendezvous point tree. • sparse—Sparse mode entry. • spt—Entry is on the shortest-path tree for the source. • wildcard—Entry is on the shared tree. 	brief detail extensive none
Upstream interface	RPF interface toward the source address for the source-specific state (S, G) or toward the rendezvous point (RP) address for the non-source-specific state (*, G).	brief detail extensive none
Upstream neighbor	Information about the upstream neighbor: Direct , Local , Unknown , or a specific IP address.	extensive

Table 29: show pim join Output Fields (*continued*)

Field Name	Field Description	Level of Output
Upstream state	Information about the upstream interface: <ul style="list-style-type: none"> • Join to RP—Sending a join to the rendezvous point. • Join to Source—Sending a join to the source. • Local RP—Sending neither joins nor prunes toward the RP, because this router is the rendezvous point. • Local Source—Sending neither joins nor prunes toward the source, because the source is locally attached to this routing device. • Prune to RP—Sending a prune to the rendezvous point. • Prune to Source—Sending a prune to the source. 	extensive
Downstream neighbors	Information about downstream interfaces: <ul style="list-style-type: none"> • Interface—Interface name for the downstream neighbor. <p>NOTE: A pseudo PIM-SM interface appears for all IGMP-only interfaces.</p> <ul style="list-style-type: none"> • Interface address—Address of the downstream neighbor. • State—Information about the downstream neighbor: join or prune. • Flags—PIM join flags: R (RPtree), S (Sparse), W (Wildcard), or zero. 	extensive
Assert Timeout	Length of time between assert cycles on downstream interface. Not displayed if assert timer is null.	extensive
Timeout	Time remaining until the downstream join state is updated (in seconds). If the downstream join state is not updated before this keepalive timer reaches zero, the entry is deleted. If there is a directly connected host, Timeout is Infinity .	extensive

Sample Output

```

show pim join summary  user@host> show pim join summary
                        Instance: PIM.master Family: INET

                        Route type      Route count
                        (s,g)           2
                        (*,g)           1

                        Instance: PIM.master Family: INET6

show pim join          user@host> show pim join

```

Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 239.1.1.1
Source: *
RP: 10.255.14.144
Flags: sparse,rptree,wildcard
Upstream interface: Local

Group: 239.1.1.1
Source: 10.255.14.144
Flags: sparse,spt
Upstream interface: Local

Group: 239.1.1.1
Source: 10.255.70.15
Flags: sparse,spt
Upstream interface: so-1/0/0.0

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

show pim join instance user@host> show pim join instance VPN-A
Instance: PIM.VPN-A Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 235.1.1.2
Source: *
RP: 10.10.47.100
Flags: sparse,rptree,wildcard
Upstream interface: Local

Group: 235.1.1.2
Source: 192.168.195.74
Flags: sparse,spt
Upstream interface: at-0/3/1.0

Group: 235.1.1.2
Source: 192.168.195.169
Flags: sparse
Upstream interface: so-1/0/1.0

Instance: PIM.VPN-A Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

show pim join detail user@host> show pim join detail
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 239.1.1.1
Source: *
RP: 10.255.14.144
Flags: sparse,rptree,wildcard
Upstream interface: Local

Group: 239.1.1.1
Source: 10.255.14.144
Flags: sparse,spt
Upstream interface: Local

Group: 239.1.1.1


```

Source: 10.255.70.15
Flags: sparse,spt
Upstream interface: so-1/0/0.0

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

show pim join extensive user@host> show pim join extensive
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 239.1.1.1
Source: *
RP: 10.255.14.144
Flags: sparse,rptree,wildcard
Upstream interface: Local
Upstream neighbor: Local
Upstream state: Local RP
Downstream neighbors:
  Interface: so-1/0/0.0
    10.111.10.2 State: Join Flags: SRW Timeout: 174
  Interface: mt-1/1/0.32768
    10.10.47.100 State: Join Flags: SRW Timeout: Infinity

Group: 239.1.1.1
Source: 10.255.14.144
Flags: sparse,spt
Upstream interface: Local
Upstream neighbor: Local
Upstream state: Local Source, Local RP
Keepalive timeout: 344
Downstream neighbors:
  Interface: so-1/0/0.0
    10.111.10.2 State: Join Flags: S Timeout: 174
  Interface: mt-1/1/0.32768
    10.10.47.100 State: Join Flags: S Timeout: Infinity

Group: 239.1.1.1
Source: 10.255.70.15
Flags: sparse,spt
Upstream interface: so-1/0/0.0
Upstream neighbor: 10.111.10.2
Upstream state: Local RP, Join to Source
Keepalive timeout: 344
Downstream neighbors:
  Interface: Pseudo-GMP
    fe-0/0/0.0 fe-0/0/1.0 fe-0/0/3.0
  Interface: so-1/0/0.0 (pruned)
    10.111.10.2 State: Prune Flags: SR Timeout: 174
  Interface: mt-1/1/0.32768
    10.10.47.100 State: Join Flags: S Timeout: Infinity

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

show pim join instance extensive user@host> show pim join instance VPN-A extensive
Instance: PIM.VPN-A Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 235.1.1.2
Source: *

```

RP: 10.10.47.100
Flags: sparse,rptree,wildcard
Upstream interface: Local
Upstream neighbor: Local
Upstream state: Local RP
Downstream neighbors:
 Interface: mt-1/1/0.32768
 10.10.47.101 State: Join Flags: SRW Timeout: 156

Group: 235.1.1.2
Source: 192.168.195.74
Flags: sparse,spt
Upstream interface: at-0/3/1.0
Upstream neighbor: 10.111.30.2
Upstream state: Local RP, Join to Source
Keepalive timeout: 156

Group: 235.1.1.2
Source: 192.168.195.169
Flags: sparse
Upstream interface: so-1/0/1.0
Upstream neighbor: 10.111.20.2
Upstream state: Local RP, Join to Source
Keepalive timeout: 156

show pim neighbors

Syntax	show pim neighbors <brief detail> <inet inet6> <instance <i>instance-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	show pim neighbors <brief detail> <inet inet6> <instance <i>instance-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Description	Display information about Protocol Independent Multicast (PIM) neighbors.
Options	<p>none—(Same as brief) Display standard information about PIM neighbors for all supported family addresses for all routing instances.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>inet inet6—(Optional) Display information about PIM neighbors for IPv4 or IPv6 family addresses, respectively.</p> <p>instance <i>instance-name</i>—(Optional) Display information about neighbors for the specified PIM-enabled routing instance.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Required Privilege Level	view
List of Sample Output	show pim neighbors on page 201 show pim neighbors brief on page 201 show pim neighbors instance on page 201 show pim neighbors detail on page 201 show pim neighbors detail (with BFD) on page 201
Output Fields	Table 30 on page 199 describes the output fields for the show pim neighbors command. Output fields are listed in the approximate order in which they appear.

Table 30: show pim neighbors Output Fields

Field Name	Field Description	Level of Output
Instance	Name of the routing instance.	All levels
Interface	Interface through which the neighbor is reachable.	All levels

Table 30: show pim neighbors Output Fields (*continued*)

Field Name	Field Description	Level of Output
Neighbor addr	Address of the neighboring PIM routing device.	All levels
IP	IP version: 4 or 6.	All levels
V	PIM version running on the neighbor: 1 or 2.	All levels
Mode	PIM mode of the neighbor: Sparse , Dense , SparseDense , or Unknown . When the neighbor is running PIM version 2, this mode is always Unknown .	All levels
Option	Can be one or more of the following: <ul style="list-style-type: none"> • B—Bidirectional Capable. • H—Hello Option Holdtime. • G—Generation Identifier. • P—Hello Option DR Priority. • L—Hello Option LAN Prune Delay. 	brief none
Uptime	Time the neighbor has been operational since the PIM process was last initialized, in the format dd:hh:mm:ss ago for less than a week and nwnd:hh:mm:ss ago for more than a week.	All levels
Address	Address of the neighboring PIM router.	detail
BFD	Status and operational state of the Bidirectional Forwarding Detection (BFD) protocol on the interface: Enabled , Operational state is up , or Disabled .	detail
Hello Option Holdtime	Time for which the neighbor is available, in seconds. The range of values is 0 through 65,535.	detail
Hello Default Holdtime	Default holdtime and the time remaining if the holdtime option is not in the received hello message.	detail
Hello Option DR Priority	Designated router election priority. The range of values is 0 through 255.	detail
Hello Option Generation ID	9- or 10-digit number used to tag hello messages.	detail
Hello Option LAN Prune Delay	Time to wait before the neighbor receives prune messages, in the format delay nnn ms override nnnn ms .	detail
Join Suppression supported	Neighbor is capable of join suppression.	detail
Rx Join	Information about joins received from the neighbor. <ul style="list-style-type: none"> • Group—Group addresses in the join message. • Source—Address of the source in the join message. • Timeout—Time for which the join is valid. 	detail

Sample Output

show pim neighbors user@host> show pim neighbors
 Instance: PIM.master
 B = Bidirectional Capable, G = Generation Identifier,
 H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
 P = Hello Option DR Priority

Interface	IP V Mode	Option	Uptime Neighbor addr
so-1/0/0.0	4 2	HPLG	00:07:10 10.111.10.2

show pim neighbors brief The output for the **show pim neighbors brief** command is identical to that for the **show pim neighbors** command. For sample output, see [show pim neighbors on page 201](#).

show pim neighbors instance user@host> show pim neighbors instance VPN-A
 Instance: PIM.VPN-A
 B = Bidirectional Capable, G = Generation Identifier,
 H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
 P = Hello Option DR Priority

Interface	IP V Mode	Option	Uptime Neighbor addr
at-0/3/1.0	4 2	HPLG	00:07:54 10.111.30.2
mt-1/1/0.32768	4 2	HPLG	00:07:22 10.10.47.101
so-1/0/1.0	4 2	HPLG	00:07:50 10.111.20.2

show pim neighbors detail user@host> show pim neighbors detail
 Instance: PIM.master
 Interface: fe-3/0/2.0
 Address: 192.168.195.37, IPv4, PIM v2, Mode: Sparse
 Hello Option Holdtime: 65535 seconds
 Hello Option DR Priority: 1
 Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
 Join Suppression supported

Rx Join: Group	Source	Timeout
225.1.1.1	192.168.195.78	0
225.1.1.1		0

Interface: lo0.0
 Address: 10.255.245.91, IPv4, PIM v2, Mode: Sparse
 Hello Option Holdtime: 65535 seconds
 Hello Option DR Priority: 1
 Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
 Join Suppression supported

Interface: pd-6/0/0.32768
 Address: 0.0.0.0, IPv4, PIM v2, Mode: Sparse
 Hello Option Holdtime: 65535 seconds
 Hello Option DR Priority: 0
 Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
 Join Suppression supported

show pim neighbors detail (with BFD) user@host> show pim neighbors detail
 Instance: PIM.master
 Interface: fe-1/0/0.0
 Address: 192.168.11.1, IPv4, PIM v2, Mode: Sparse
 Hello Option Holdtime: 65535 seconds
 Hello Option DR Priority: 1
 Hello Option Generation ID: 836607909
 Hello Option LAN Prune Delay: delay 500 ms override 2000 ms

```
Address: 192.168.11.2,      IPv4, PIM v2
  BFD: Enabled, Operational state is up
  Hello Default Holdtime: 105 seconds 104 remaining
  Hello Option DR Priority: 1
  Hello Option Generation ID: 1907549685
  Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
```

```
Interface: fe-1/0/1.0
  Address: 192.168.12.1,      IPv4, PIM v2
    BFD: Disabled
    Hello Default Holdtime: 105 seconds 80 remaining
    Hello Option DR Priority: 1
    Hello Option Generation ID: 1971554705
    Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
```

show pim rps

Syntax	<pre>show pim rps <brief detail extensive> <group-address> <inet inet6> <instance instance-name> <logical-system (all logical-system-name)></pre>
Syntax (EX Series Switch)	<pre>show pim rps <brief detail extensive> <group-address> <inet inet6> <instance instance-name></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.</p>
Description	Display information about Protocol Independent Multicast (PIM) rendezvous points (RPs).
Options	<p>none—Display standard information about PIM RPs for all groups and family addresses for all routing instances.</p> <p>brief detail extensive—(Optional) Display the specified level of output.</p> <p>group-address—(Optional) Display the RPs for a particular group. If you specify a group address, the output lists the routing device that is the RP for that group.</p> <p>inet inet6—(Optional) Display information for IPv4 or IPv6 family addresses, respectively.</p> <p>instance instance-name—(Optional) Display information about RPs for a specific PIM-enabled routing instance.</p> <p>logical-system (all logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Required Privilege Level	view
List of Sample Output	<p>show pim rps on page 205</p> <p>show pim rps brief on page 205</p> <p>show pim rps instance on page 206</p> <p>show pim rps extensive on page 206</p> <p>show pim rps extensive (PIM Anycast RP in Use) on page 206</p>
Output Fields	Table 31 on page 204 describes the output fields for the show pim rps command. Output fields are listed in the approximate order in which they appear.

Table 31: show pim rps Output Fields

Field Name	Field Description	Level of Output
Instance	Name of the routing instance.	All levels
Family	Name of the address family: inet (IPv4) or inet6 (IPv6).	All levels
RP address	Address of the rendezvous point.	All levels
Type	Type of RP: <ul style="list-style-type: none"> • auto-rp—Address of the RP known through the Auto-RP protocol. • bootstrap—Address of the RP known through the bootstrap router protocol (BSR). • embedded—Address of the RP known through an embedded RP (IPv6). • static—Address of RP known through static configuration. 	brief none
Holdtime	How long to keep the RP active, with time remaining, in seconds.	All levels
Timeout	How long until the local routing device determines the RP to be unreachable, in seconds.	All levels
Groups	Number of groups currently using this RP.	All levels
Group prefixes	Addresses of groups that this RP can span.	brief none
Learned via	Address and method by which the RP was learned.	detail extensive
Time Active	How long the RP has been active, in the format <i>hh:mm:ss</i> .	detail extensive
Device Index	Index value of the order in which the Junos OS finds and initializes the interface.	detail extensive
Subunit	Logical unit number of the interface.	detail extensive
Interface	Either the encapsulation or the de-encapsulation logical interface, depending on whether this routing device is a designated router (DR) facing an RP router, or is the local RP, respectively.	detail extensive
Group Ranges	Addresses of groups that this RP spans.	detail extensive
Active groups using RP	Number of groups currently using this RP.	detail extensive
total	Total number of active groups for this RP.	detail extensive

Table 31: show pim rps Output Fields (*continued*)

Field Name	Field Description	Level of Output
Register State for RP	<p>Current register state for each group:</p> <ul style="list-style-type: none"> • Group—Multicast group address. • Source—Multicast source address for which the PIM register is sent or received, depending on whether this router is a designated router facing an RP router, or is the local RP, respectively: • First Hop—PIM-designated routing device that sent the Register message (the source address in the IP header). • RP Address—RP to which the Register message was sent (the destination address in the IP header). • State: <ul style="list-style-type: none"> On the designated router: <ul style="list-style-type: none"> • Send—Sending Register messages. • Probe—Sent a null register. If a Register-Stop message does not arrive in 5 seconds, the designated router resumes sending Register messages. • Suppress—Received a Register-Stop message. The designated router is waiting for the timer to resume before changing to Probe state. On the RP: <ul style="list-style-type: none"> • Receive—Receiving Register messages. 	extensive
Anycast-PIM rpset	If anycast RP is configured, the addresses of the RPs in the set.	extensive
Anycast-PIM local address used	If anycast RP is configured, the local address used by the RP.	extensive
Anycast-PIM Register State	<p>If anycast RP is configured, the current register state for each group:</p> <ul style="list-style-type: none"> • Group—Multicast group address. • Source—Multicast source address for which the PIM register is sent or received, depending on whether this routing device is a designated router facing an RP router, or is the local RP, respectively. • Origin—How the information was obtained: <ul style="list-style-type: none"> • DIRECT—From a local attachment • MSDP—From the Multicast Source Discovery Protocol (MSDP) • DR—From the designated router 	extensive

Sample Output

```

show pim rps user@host> show pim rps
Instance: PIM.master
Address family INET
RP address      Type      Holdtime Timeout Groups Group prefixes
10.255.14.144   static    0        None      1 224.0.0.0/4

Address family INET6

```

show pim rps brief The output for the **show pim rps brief** command is identical to that for the **show pim rps** command. For sample output, see [show pim rps on page 205](#).

```

show pim rps instance user@host> show pim rps instance VPN-A
Instance: PIM.VPN-A
Address family INET
RP address          Type          Holdtime Timeout Groups Group prefixes
10.10.47.100        static          0      None      1 224.0.0.0/4

Address family INET6

show pim rps extensive user@host> show pim rps extensive
Instance: PIM.master

Family: INET
RP: 10.255.245.91
Learned via: static configuration
Time Active: 00:05:48
Holdtime: 45 with 36 remaining
Device Index: 122
Subunit: 32768
Interface: pd-6/0/0.32768
Group Ranges:
    224.0.0.0/4, 36s remaining
Active groups using RP:
    225.1.1.1

    total 1 groups active

Register State for RP:
Group          Source          FirstHop          RP Address          State          Timeout
225.1.1.1      192.168.195.78  10.255.14.132    10.255.245.91      Receive        0

show pim rps extensive user@host> show pim rps extensive
(PIM Anycast RP in Instance: PIM.master
Use)
Family: INET
RP: 10.10.10.2
Learned via: static configuration
Time Active: 00:54:52
Holdtime: 0
Device Index: 130
Subunit: 32769
Interface: pimd.32769
Group Ranges:
    224.0.0.0/4
Active groups using RP:
    224.10.10.10

    total 1 groups active

Anycast-PIM rpset:
    10.100.111.34
    10.100.111.17
    10.100.111.55

Anycast-PIM local address used: 10.100.111.1
Anycast-PIM Register State:
Group          Source          Origin
224.1.1.1      10.10.95.2      DIRECT
224.1.1.2      10.10.95.2      DIRECT
224.10.10.10   10.10.70.1      MSDP
224.10.10.11   10.10.70.1      MSDP

```

224.20.20.1 10.10.71.1 DR

Address family INET6

Anycast-PIM rpset:

 ab::1

 ab::2

Anycast-PIM local address used: cd::1

Anycast-PIM Register State:

Group	Source	Origin
::224.1.1.1	::10.10.95.2	DIRECT
::224.1.1.2	::10.10.95.2	DIRECT
::224.20.20.1	::10.10.71.1	DR

show pim source

Syntax	<pre>show pim source <brief detail> <inet inet6> <instance <i>instance-name</i>> <logical-system (all <i>logical-system-name</i>)> <source-prefix></pre>
Syntax (EX Series Switch)	<pre>show pim source <brief detail> <inet inet6> <instance <i>instance-name</i>> <source-prefix></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.</p>
Description	Display information about the Protocol Independent Multicast (PIM) source reverse path forwarding (RPF) state.
Options	<p>none—Display standard information about the PIM RPF state for all supported family addresses for all routing instances.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>inet inet6—(Optional) Display information for IPv4 or IPv6 family addresses, respectively.</p> <p>instance <i>instance-name</i>—(Optional) Display information about the RPF state for a specific PIM-enabled routing instance.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> <p>source-prefix—(Optional) Display the state for source RPF states in the given range.</p>
Required Privilege Level	view
List of Sample Output	show pim source on page 209 show pim source brief on page 209 show pim source detail on page 209
Output Fields	<p>Table 32 on page 208 describes the output fields for the show pim source command. Output fields are listed in the approximate order in which they appear.</p>

Table 32: show pim source Output Fields

Field Name	Field Description
Instance	Name of the routing instance.

Table 32: show pim source Output Fields (*continued*)

Field Name	Field Description
RPF Address	Address of the source or reverse path.
Prefix/length	Prefix and prefix length for the route used to reach the RPF address.
Upstream interface	RPF interface toward the source address.
Neighbor address	Address of the RPF neighbor used to reach the source address.

Sample Output

```

show pim source user@host> show pim source
Instance: PIM.master Family: INET

Source 10.255.14.144
  Prefix 10.255.14.144/32
  Upstream interface Local
  Upstream neighbor Local

Source 10.255.70.15
  Prefix 10.255.70.15/32
  Upstream interface so-1/0/0.0
  Upstream neighbor 10.111.10.2

Instance: PIM.master Family: INET6

```

show pim source brief The output for the **show pim source brief** command is identical to that for the **show pim source** command. For sample output, see [show pim source on page 209](#).

```

show pim source detail user@host> show pim source detail
Instance: PIM.master Family: INET

Source 10.255.14.144
  Prefix 10.255.14.144/32
  Upstream interface Local
  Upstream neighbor Local
  Active groups:228.0.0.0
    239.1.1.1
    239.1.1.1

Source 10.255.70.15
  Prefix 10.255.70.15/32
  Upstream interface so-1/0/0.0
  Upstream neighbor 10.111.10.2
  Active groups:239.1.1.1

Instance: PIM.master Family: INET6

```

show pim statistics

Syntax	show pim statistics <inet inet6> <instance <i>instance-name</i> > <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch)	show pim statistics <inet inet6> <instance <i>instance-name</i> > <interface <i>interface-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Description	Display Protocol Independent Multicast (PIM) statistics.
Options	none—Display PIM statistics. inet inet6—(Optional) Display IPv4 or IPv6 PIM statistics. instance <i>instance-name</i> —(Optional) Display statistics for a specific routing instance enabled by Protocol Independent Multicast (PIM). interface <i>interface-name</i> —(Optional) Display statistics about the specified interface. logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• clear pim statistics on page 129
List of Sample Output	show pim statistics on page 216 show pim statistics inet interface interface-name on page 217 show pim statistics inet6 interface interface-name on page 217 show pim statistics interface interface-name on page 218
Output Fields	Table 33 on page 211 describes the output fields for the show pim statistics command. Output fields are listed in the approximate order in which they appear.

Table 33: show pim statistics Output Fields

Field Name	Field Description
Instance	<p>Name of the routing instance.</p> <p>This field only appears if you specify an interface, for example:</p> <ul style="list-style-type: none"> • inet interface <i>interface-name</i> • inet6 interface <i>interface-name</i> • interface <i>interface-name</i>
Family	<p>Output is for IPv4 or IPv6 PIM statistics. INET indicates IPv4 statistics, and INET6 indicates IPv6 statistics.</p> <p>This field only appears if you specify an interface, for example:</p> <ul style="list-style-type: none"> • inet interface <i>interface-name</i> • inet6 interface <i>interface-name</i> • interface <i>interface-name</i>
PIM statistics	PIM statistics for all interfaces or for the specified interface.
PIM message type	Message type for which statistics are displayed.
Received	Number of received statistics.
Sent	Number of messages sent of a certain type.
Rx errors	Number of received packets that contained errors.
V2 Hello	PIM version 2 hello packets.
V2 Register	PIM version 2 register packets.
V2 Register Stop	PIM version 2 register stop packets.
V2 Join Prune	PIM version 2 join and prune packets.
V2 Bootstrap	PIM version 2 bootstrap packets.
V2 Assert	PIM version 2 assert packets.
V2 Graft	PIM version 2 graft packets.
V2 Graft Ack	PIM version 2 graft acknowledgement packets.
V2 Candidate RP	PIM version 2 candidate RP packets.
V1 Query	PIM version 1 query packets.
V1 Register	PIM version 1 register packets.

Table 33: show pim statistics Output Fields (*continued*)

Field Name	Field Description
V1 Register Stop	PIM version 1 register stop packets.
V1 Join Prune	PIM version 1 join and prune packets.
V1 RP Reachability	PIM version 1 RP reachability packets.
V1 Assert	PIM version 1 assert packets.
V1 Graft	PIM version 1 graft packets.
V1 Graft Ack	PIM version 1 graft acknowledgement packets.
AutoRP Announce	Auto-RP announce packets.
AutoRP Mapping	Auto-RP mapping packets.
AutoRP Unknown type	Auto-RP packets with an unknown type.
Anycast Register	Auto-RP announce packets.
Anycast Register Stop	Auto-RP announce packets.
Global Statistics	Summary of PIM statistics for all interfaces.
Hello dropped on neighbor policy	Number of hello packets dropped because of a configured neighbor policy.
Unknown type	Number of PIM control packets received with an unknown type.
V1 Unknown type	Number of PIM version 1 control packets received with an unknown type.
Unknown Version	Number of PIM control packets received with an unknown version. The version is not version 1 or version 2.
Neighbor unknown	Number of PIM control packets received (excluding PIM hello) without first receiving the hello packet.
Bad Length	Number of PIM control packets received for which the packet size does not match the PIM length field in the packet.
Bad Checksum	Number of PIM control packets received for which the calculated checksum does not match the checksum field in the packet.
Bad Receive If	Number of PIM control packets received on an interface that does not have PIM configured.

Table 33: show pim statistics Output Fields (*continued*)

Field Name	Field Description
Rx Bad Data	Number of PIM control packets received that contain data for TCP. Bad register packets.
Rx Intf disabled	Number of PIM control packets received on an interface that has PIM disabled.
Rx V1 Require V2	Number of PIM version 1 control packets received on an interface configured for PIM version 2.
Rx V2 Require V1	Number of PIM version 2 control packets received on an interface configured for PIM version 1.
Rx Register not RP	Number of PIM register packets received when the router is not the RP for the group.
Rx Register no route	Number of PIM register packets received when the RP does not have a unicast route back to source.
Rx Register no decap if	Number of PIM register packets received when the RP does not have a de-encapsulation interface.
Null Register Timeout	Number of NULL register timeout packets.
RP Filtered Source	Number of PIM packets received when the router has a source address filter configured for the RP.
Rx Unknown Reg Stop	Number of register stop messages with an unknown type.
Rx Join/Prune no state	Number of join and prune messages received for which the router has no state.
Rx Join/Prune on upstream if	Number of join and prune messages received on the interface used to reach the upstream router, toward the RP.
Rx Join/Prune messages dropped	Number of join and prune messages received and dropped.
Rx sparse join for dense group	Number of PIM sparse mode join messages received for a group that is configured for dense mode.
Rx Graft/Graft Ack no state	Number of graft and graft acknowledgement messages received for which the router has no state.
Rx Graft on upstream if	Number of graft messages received on the interface used to reach the upstream router, toward the RP.
Rx CRP not BSR	Number of BSR messages received in which the PIM message type is Candidate-RP-Advertisement, not Bootstrap.

Table 33: show pim statistics Output Fields (*continued*)

Field Name	Field Description
Rx BSR when BSR	Number of BSR messages received in which the PIM message type is Bootstrap.
Rx BSR not RPF if	Number of BSR messages received on an interface that is not the RPF interface.
Rx unknown hello opt	Number of PIM hello packets received with options that Junos does not support.
Rx data no state	Number of PIM control packets received for which the router has no state for the data type.
Rx RP no state	Number of PIM control packets received for which the router has no state for the RP.
Rx aggregate	Number of PIM aggregate MDT packets received.
Rx malformed packet	Number of PIM control packets received with a malformed IP unicast or multicast address family.
No RP	Number of PIM control packets received with no RP address.
No register encap if	Number of PIM register packets received when the first-hop router does not have an encapsulation interface.
No route upstream	Number of PIM control packets received when the router does not have a unicast route to the the interface used to reach the upstream router, toward the RP.
Nexthop Unusable	Number of PIM control packets with an unusable nexthop. A path can be unusable if the route is hidden or the link is down.
RP mismatch	Number of PIM control packets received for which the router has an RP mismatch.
RPF neighbor unknown	Number of PIM control packets received for which the router has an unknown RPF neighbor for the source.
Rx Joins/Prunes filtered	The number of join and prune messages filtered because of configured route filters and source address filters.
Tx Joins/Prunes filtered	The number of join and prune messages filtered because of configured route filters and source address filters.
Embedded-RP invalid addr	Number of packets received with an invalid embedded RP address in PIM join messages and other types of messages sent between routing domains.

Table 33: show pim statistics Output Fields (*continued*)

Field Name	Field Description
Embedded-RP limit exceed	Number of times the limit configure with the maximum-rps statement is exceeded. The maximum-rps statement limits the number of embedded RPs created in a specific routing instance. The range is from 1 through 500. The default is 100.
Embedded-RP added	<p>Number of packets in which the embedded RP for IPv6 is added.</p> <p>The following receive events trigger extraction of an IPv6 embedded RP address on the router:</p> <ul style="list-style-type: none"> • Multicast Listener Discovery (MLD) report for an embedded RP multicast group address • PIM join message with an embedded RP multicast group address • Static embedded RP multicast group address associated with an interface • Packets sent to an embedded RP multicast group address received on the DR <p>An embedded RP node discovered through these receive events is added if it does not already exist on the routing platform.</p>
Embedded-RP removed	Number of packets in which the embedded RP for IPv6 is removed. The embedded RP is removed whenever all PIM join states using this RP are removed or the configuration changes to remove the embedded RP feature.
Rx Register msgs filtering drop	Number of register messages dropped because of a filter configured for PIM register messages.
Tx Register msgs filtering drop	Number of register messages dropped because of a filter configured for PIM register messages.

Sample Output

```

show pim statistics user@host> show pim statistics
PIM Message type      Received      Sent  Rx errors
V2 Hello               15           32      0
V2 Register            0          362      0
V2 Register Stop       483           0      0
V2 Join Prune          18          518      0
V2 Bootstrap           0            0      0
V2 Assert              0            0      0
V2 Graft               0            0      0
V2 Graft Ack           0            0      0
V2 Candidate RP        0            0      0
V1 Query               0            0      0
V1 Register            0            0      0
V1 Register Stop       0            0      0
V1 Join Prune          0            0      0
V1 RP Reachability     0            0      0
V1 Assert              0            0      0
V1 Graft               0            0      0
V1 Graft Ack           0            0      0
AutoRP Announce        0            0      0
AutoRP Mapping         0            0      0
AutoRP Unknown type    0            0      0
Anycast Register       0            0      0
Anycast Register Stop  0            0      0

```

Global Statistics

```

Hello dropped on neighbor policy 0
Unknown type                     0
V1 Unknown type                  0
Unknown Version                  0
Neighbor unknown                 5
Bad Length                       0
Bad Checksum                     0
Bad Receive If                   0
Rx Bad Data                      0
Rx Intf disabled                 0
Rx V1 Require V2                 0
Rx V2 Require V1                 0
Rx Register not RP               0
Rx Register no route             0
Rx Register no decap if          0
Null Register Timeout            0
RP Filtered Source               0
Rx Unknown Reg Stop              0
Rx Join/Prune no state           0
Rx Join/Prune on upstream if     0
Rx Join/Prune messages dropped   0
Rx sparse join for dense group   0
Rx Graft/Graft Ack no state      0
Rx Graft on upstream if         0
Rx CRP not BSR                  0
Rx BSR when BSR                  0
Rx BSR not RPF if                0
Rx unknown hello opt             0
Rx data no state                 0

```

```

Rx RP no state          0
Rx aggregate            0
Rx malformed packet     0
No RP                   0
No register encap if    0
No route upstream       0
Nexthop Unusable       0
RP mismatch             0
RPF neighbor unknown    0
Rx Joins/Prunes filtered 0
Embedded-RP invalid addr 0
Embedded-RP limit exceed 0
Embedded-RP added       0
Embedded-RP removed     0
Rx Register msgs filtering drop 0
Tx Register msgs filtering drop 0

```

Sample Output

```

show pim statistics user@host> show pim statistics inet interface ge-0/3/0.0
inet interface      Instance: PIM.master Family: INET
interface-name      PIM Interface statistics for ge-0/3/0.0

```

PIM Message type	Received	Sent	Rx errors
V2 Hello	0	4	0
V2 Register	0	0	0
V2 Register Stop	0	0	0
V2 Join Prune	0	0	0
V2 Bootstrap	0	0	0
V2 Assert	0	0	0
V2 Graft	0	0	0
V2 Graft Ack	0	0	0
V2 Candidate RP	0	0	0
V1 Query	0	0	0
V1 Register	0	0	0
V1 Register Stop	0	0	0
V1 Join Prune	0	0	0
V1 RP Reachability	0	0	0
V1 Assert	0	0	0
V1 Graft	0	0	0
V1 Graft Ack	0	0	0
AutoRP Announce	0	0	0
AutoRP Mapping	0	0	0
AutoRP Unknown type	0		
Anycast Register	0	0	0
Anycast Register Stop	0	0	0

Sample Output

```

show pim statistics user@host> show pim statistics inet6 interface ge-0/3/0.0
inet6 interface     Instance: PIM.master Family: INET6
interface-name      PIM Interface statistics for ge-0/3/0.0

```

PIM Message type	Received	Sent	Rx errors
V2 Hello	0	4	0
V2 Register	0	0	0
V2 Register Stop	0	0	0
V2 Join Prune	0	0	0

V2 Bootstrap	0	0	0
V2 Assert	0	0	0
V2 Graft	0	0	0
V2 Graft Ack	0	0	0
V2 Candidate RP	0	0	0
Anycast Register	0	0	0
Anycast Register Stop	0	0	0

Sample Output

```
show pim statistics user@host> show pim statistics interface ge-0/3/0.0
interface          Instance: PIM.master Family: INET
```

```
interface-name      PIM Interface statistics for ge-0/3/0.0
```

PIM Message type	Received	Sent	Rx errors
V2 Hello	0	3	0
V2 Register	0	0	0
V2 Register Stop	0	0	0
V2 Join Prune	0	0	0
V2 Bootstrap	0	0	0
V2 Assert	0	0	0
V2 Graft	0	0	0
V2 Graft Ack	0	0	0
V2 Candidate RP	0	0	0
V1 Query	0	0	0
V1 Register	0	0	0
V1 Register Stop	0	0	0
V1 Join Prune	0	0	0
V1 RP Reachability	0	0	0
V1 Assert	0	0	0
V1 Graft	0	0	0
V1 Graft Ack	0	0	0
AutoRP Announce	0	0	0
AutoRP Mapping	0	0	0
AutoRP Unknown type	0		
Anycast Register	0	0	0
Anycast Register Stop	0	0	0

```
Instance: PIM.master Family: INET6
```

```
PIM Interface statistics for ge-0/3/0.0
```

PIM Message type	Received	Sent	Rx errors
V2 Hello	0	3	0
V2 Register	0	0	0
V2 Register Stop	0	0	0
V2 Join Prune	0	0	0
V2 Bootstrap	0	0	0
V2 Assert	0	0	0
V2 Graft	0	0	0
V2 Graft Ack	0	0	0
V2 Candidate RP	0	0	0
Anycast Register	0	0	0
Anycast Register Stop	0	0	0