

Multicast Feature Guide for EX2300, EX3400, and EX4300 Switches

Release
15.1



Modified: 2016-07-04

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

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.

Multicast Feature Guide for EX2300, EX3400, and EX4300 Switches
Release 15.1
Copyright © 2016, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

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 the Documentation	xi
	Documentation and Release Notes	xi
	Supported Platforms	xi
	Using the Examples in This Manual	xi
	Merging a Full Example	xii
	Merging a Snippet	xii
	Documentation Conventions	xiii
	Documentation Feedback	xv
	Requesting Technical Support	xv
	Self-Help Online Tools and Resources	xv
	Opening a Case with JTAC	xvi
Chapter 1	Configuring IGMP Snooping to Constrain Flooding of Multicast Traffic . . .	17
	IGMP Snooping on EX Series Switches Overview	17
	How IGMP Snooping Works	18
	IGMP Message Types	18
	How Hosts Join and Leave Multicast Groups	19
	Support for IGMPv3 Multicast Sources	19
	IGMP Snooping and Forwarding Interfaces	20
	General Forwarding Rules	21
	Examples of IGMP Snooping Multicast Forwarding	21
	Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts	21
	Scenario 2: Switch Forwarding Multicast Traffic to Another Switch	22
	Scenario 3: Switch Connected to Hosts Only (No IGMP Querier)	23
	Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs	24
	Configuring IGMP Snooping (CLI Procedure)	25
	Enabling IGMP Snooping on VLANs	26
	Enabling Immediate Leave	26
	Configuring an Interface as a Multicast-Router Interface	27
	Configuring Static Group Membership on an Interface	28
	Changing the Timer and Counter Values	29
	Configuring IGMP Snooping (J-Web Procedure)	30
	Example: Configuring IGMP Snooping	32
	Configuring IGMP Snooping Tracing Operations (CLI Procedure)	36
	Configuring Tracing Operations	37
	Viewing, Stopping, and Restarting Tracing Operations	37
	Verifying IGMP Snooping (CLI Procedure)	38
	Verifying IGMP Snooping Memberships	38
	Viewing IGMP Snooping Statistics	39

Chapter 2

Viewing IGMP Snooping Routing Information	39
Monitoring IGMP Snooping	40
Configuration Statements	45
[edit protocols] Configuration Statement Hierarchy on EX Series Switches	47
[edit protocols igmp-snooping] Configuration Statement Hierarchy	48
Supported Statements in the [edit protocols igmp-snooping] Hierarchy	
Level	49
Unsupported Statements in the [edit protocols igmp-snooping] Hierarchy	
Level	49
accounting (Protocols IGMP Interface)	50
accounting (Protocols IGMP)	50
address (Anycast RPs)	51
address (Local RPs)	52
anycast-pim	53
assert-timeout	54
auto-rp	55
bootstrap	56
bootstrap-export	57
bootstrap-import	58
bootstrap-priority	59
data-forwarding	60
dense-groups	61
disable (IGMP Snooping)	61
disable (Protocols IGMP)	62
disable (PIM)	63
dr-election-on-p2p	64
dr-register-policy	64
embedded-rp	65
export (Bootstrap)	66
family (Bootstrap)	67
family (Local RP)	68
graceful-restart (Protocols PIM)	69
group (IGMP Snooping)	69
group (Protocols IGMP)	70
group-ranges	71
hello-interval	72
hold-time (Protocols PIM)	73
igmp-snooping	74
immediate-leave (Protocols IGMP)	75
immediate-leave (IGMP Snooping)	76
import (Protocols PIM Bootstrap)	77
import (Protocols PIM)	78
infinity	79
interface (IGMP Snooping)	80
interface (Protocols PIM)	81
interface (Protocols IGMP)	83
join-load-balance	84
local	85

local-address (Protocols PIM)	86
mapping-agent-election	87
maximum-rps	88
mode (Protocols PIM)	89
multicast-router-interface (IGMP Snooping)	90
neighbor-policy	91
pim	92
priority (PIM Interfaces)	96
priority (Bootstrap)	97
priority (PIM RPs)	98
query-interval (Protocols IGMP)	99
query-last-member-interval (Protocols IGMP)	100
query-response-interval (Protocols IGMP)	101
receiver	102
register-probe-time	102
restart-duration (Protocols PIM)	103
rib-group (Protocols PIM)	104
robust-count (IGMP Snooping)	105
robust-count (Protocols IGMP)	105
rp	106
rp-register-policy	108
rp-set	109
source (Protocols IGMP)	110
source-vlans	111
spt-threshold	112
ssm-map (Protocols IGMP)	113
static (IGMP Snooping)	113
static (Protocols PIM)	114
static (Protocols IGMP)	115
traceoptions (Protocols PIM)	116
traceoptions (Protocols IGMP)	119
traceoptions (IGMP Snooping)	122
version (Protocols IGMP)	124
version (IGMP Snooping)	125
version (PIM)	126
vlan (IGMP Snooping)	127
Chapter 3 Operational Commands	129
clear igmp membership	131
clear igmp statistics	134
clear igmp-snooping membership	136
clear igmp-snooping statistics	137
clear multicast bandwidth-admission	138
clear multicast scope	140
clear multicast sessions	141
clear multicast statistics	142
clear pim join	143
clear pim register	145
clear pim statistics	147

mtrace	150
mtrace from-source	153
mtrace monitor	156
mtrace to-gateway	158
show igmp group	161
show igmp interface	165
show igmp statistics	169
show igmp-snooping membership	172
show igmp-snooping route	175
show igmp-snooping statistics	177
show multicast flow-map	179
show multicast interface	181
show multicast mrinfo	183
show multicast next-hops	185
show multicast pim-to-igmp-proxy	188
show multicast pim-to-mld-proxy	190
show multicast route	192
show multicast rpf	198
show multicast scope	202
show multicast sessions	204
show multicast usage	207
show pim bootstrap	210
show pim interfaces	212
show pim join	215
show pim neighbors	236
show pim rps	240
show pim source	247
show pim statistics	250

List of Figures

Chapter 1	Configuring IGMP Snooping to Constrain Flooding of Multicast Traffic . . .	17
	Figure 1: Multicast Traffic Flow with IGMP Snooping Enabled	18
	Figure 2: Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts	22
	Figure 3: Scenario 2: Switch Forwarding Multicast Traffic to Another Switch	23
	Figure 4: Scenario 3: Switch Connected to Hosts Only (No IGMP Querier)	24
	Figure 5: Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs	25
	Figure 6: IGMP Snooping Topology Sample Topology	34

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xiii
	Table 2: Text and Syntax Conventions	xiii
Chapter 1	Configuring IGMP Snooping to Constrain Flooding of Multicast Traffic . . .	17
	Table 3: IGMP Snooping Configuration Fields	31
	Table 4: Supported Tracing Operations for IGMP Snooping	36
	Table 5: Summary of IGMP Snooping Output Fields	41
Chapter 3	Operational Commands	129
	Table 6: mtrace Output Fields	150
	Table 7: mtrace from-source Output Fields	154
	Table 8: mtrace monitor Output Fields	156
	Table 9: mtrace to-gateway Output Fields	159
	Table 10: show igmp group Output Fields	161
	Table 11: show igmp interface Output Fields	165
	Table 12: show igmp statistics Output Fields	169
	Table 13: show igmp-snooping membership Output Fields	172
	Table 14: show igmp-snooping route Output Fields	175
	Table 15: show igmp-snooping statistics Output Fields	177
	Table 16: show multicast flow-map Output Fields	179
	Table 17: show multicast interface Output Fields	181
	Table 18: show multicast minfo Output Fields	183
	Table 19: show multicast next-hops Output Fields	186
	Table 20: show multicast pim-to-igmp-proxy Output Fields	188
	Table 21: show multicast pim-to-mld-proxy Output Fields	190
	Table 22: show multicast route Output Fields	193
	Table 23: show multicast rpf Output Fields	199
	Table 24: show multicast scope Output Fields	202
	Table 25: show multicast sessions Output Fields	204
	Table 26: show multicast usage Output Fields	208
	Table 27: show pim bootstrap Output Fields	210
	Table 28: show pim interfaces Output Fields	212
	Table 29: show pim join Output Fields	217
	Table 30: show pim neighbors Output Fields	237
	Table 31: show pim rps Output Fields	241
	Table 32: show pim source Output Fields	248
	Table 33: show pim statistics Output Fields	251

About the Documentation

- Documentation and Release Notes on page xi
- Supported Platforms on page xi
- Using the Examples in This Manual on page xi
- Documentation Conventions on page xiii
- Documentation Feedback on page xv
- Requesting Technical Support on page xv

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- EX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xiii defines notice icons used in this guide.

Table 1: 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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xiii defines the text and syntax conventions used in this guide.

Table 2: 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

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none">Introduces or emphasizes important new terms.Identifies guide 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 CLI User 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>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents 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.

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu 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. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

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 Partner Support Service 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:
<http://kb.juniper.net/InfoCenter/>
- 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>.

CHAPTER 1

Configuring IGMP Snooping to Constrain Flooding of Multicast Traffic

- [IGMP Snooping on EX Series Switches Overview on page 17](#)
- [Configuring IGMP Snooping \(CLI Procedure\) on page 25](#)
- [Configuring IGMP Snooping \(J-Web Procedure\) on page 30](#)
- [Example: Configuring IGMP Snooping on page 32](#)
- [Configuring IGMP Snooping Tracing Operations \(CLI Procedure\) on page 36](#)
- [Verifying IGMP Snooping \(CLI Procedure\) on page 38](#)
- [Monitoring IGMP Snooping on page 40](#)

IGMP Snooping on EX Series Switches Overview

Internet Group Management Protocol (IGMP) snooping constrains the flooding of IPv4 multicast traffic on VLANs on a switch. When IGMP snooping is enabled on a VLAN, a Juniper Networks EX Series Ethernet Switch examines IGMP messages between hosts and multicast routers and learns which hosts are interested in receiving traffic for a multicast group. Based on what it learns, the switch then forwards multicast traffic only to those interfaces in the VLAN that are connected to interested receivers instead of flooding the traffic to all interfaces.

IGMP snooping on EX Series switches supports IGMP version 1 (IGMPv1), IGMPv2, and IGMPv3. For details on IGMP, see the following standards:

- IGMPv1—See RFC 1112, *Host extensions for IP multicasting*.
- IGMPv2—See RFC 2236, *Internet Group Management Protocol, Version 2*.
- For IGMPv3—See RFC 3376, *Internet Group Management Protocol, Version 3*.

This topic covers:

- [How IGMP Snooping Works on page 18](#)
- [IGMP Message Types on page 18](#)
- [How Hosts Join and Leave Multicast Groups on page 19](#)
- [Support for IGMPv3 Multicast Sources on page 19](#)
- [IGMP Snooping and Forwarding Interfaces on page 20](#)

- [General Forwarding Rules on page 21](#)
- [Examples of IGMP Snooping Multicast Forwarding on page 21](#)

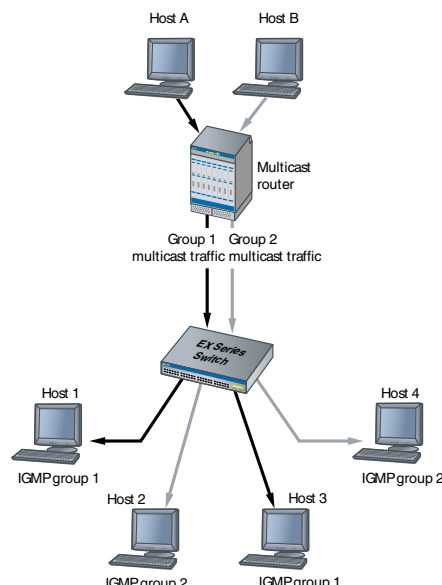
How IGMP Snooping Works

A Layer 2 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.

You can enable IGMP snooping on a switch to avoid this flooding. When IGMP snooping is enabled, the switch monitors IGMP messages between receivers and multicast routers and uses the content of the messages to build an IPv4 multicast forwarding table—a database of multicast groups and the interfaces that are connected to members of the groups. When the switch receives multicast traffic for a multicast group, it uses the forwarding table to forward the traffic only to interfaces that are connected to receivers that belong to the multicast group.

[Figure 1 on page 18](#) shows an example of multicast traffic flow with IGMP snooping enabled.

Figure 1: Multicast Traffic Flow with IGMP Snooping Enabled



IGMP Message Types

Multicast routers use IGMP to learn, for each of their attached physical networks, which groups have interested listeners. In any given subnet, one multicast router acts as an IGMP querier. The IGMP querier sends out the following types of queries to hosts:

- General query—Asks whether any host is listening to any group.

- Group-specific query—(IGMPv2 and IGMPv3 only) Asks whether any host is listening to a specific multicast group. This query is sent in response to a host leaving the multicast group and allows the router to quickly determine if any remaining hosts are interested in the group.
- Group-and-source-specific query—(IGMPv3 only) Asks whether any host is listening to group multicast traffic from a specific multicast source. This query is sent in response to a host indicating that it is not longer interested in receiving group multicast traffic from the multicast source and allows the router to quickly determine any remaining hosts are interested in receiving group multicast traffic from that source.

Hosts that are multicast listeners send the following kinds of messages:

- Membership report—Indicates that the host wants to join a particular multicast group.
- Leave report—(IGMPv2 and IGMPv3 only) Indicates that the host wants to leave a particular multicast group.

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.

Hosts can leave a multicast group in either of two ways:

- By not responding to periodic queries within a set interval of time. This results in what is known as a “silent leave.” This is the only method available to IGMPv1 hosts.
- By sending a leave report. This method can be used by IGMPv2 and IGMPv3 hosts.



NOTE: If a host is connected to the switch through a hub, the host does not automatically leave the multicast group if it disconnects from the hub. The host remains a member of the group until group membership times out and a silent leave occurs. If another host connects to the hub port before the silent leave occurs, the new host might receive the group multicast traffic until the silent leave, even though it never sent an membership report.

Support for IGMPv3 Multicast Sources

In IGMPv3, a host can send a membership report that includes a list of source addresses. When the host sends a membership report in INCLUDE mode, the host is interested in

group multicast traffic only from those sources in the source address list. If host sends a membership report in EXCLUDE mode, the host is interested in group multicast traffic from any source *except* the sources in the source address list. 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.

EX Series switches support IGMPv3 membership reports that are in INCLUDE and EXCLUDE mode. However, EX Series switches do not support forwarding on a per-source basis. Instead, a switch consolidates all INCLUDE and EXCLUDE mode reports it receives on a VLAN for a specified group into a single route that includes all multicast sources for that group, with the next hop being all interfaces that have interested receivers for the group. As a result, interested receivers on the VLAN can receive traffic from a source that they did not include in their INCLUDE report or from a source they excluded in their EXCLUDE report. For example, if Host 1 wants traffic for G from Source A and Host 2 wants traffic for G from Source B, they both receive traffic for G regardless of whether A or B sends the traffic.

IGMP Snooping and Forwarding Interfaces

To determine how to forward multicast traffic, a switch with IGMP snooping enabled maintains information about the following interfaces in its multicast forwarding 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.

The switch learns about these interfaces by monitoring IGMP traffic. If an interface receives IGMP queries or Protocol Independent Multicast (PIM) updates, the switch adds the interface to its multicast forwarding table as a multicast-router interface. If an interface receives membership reports for a multicast group, the switch adds the interface to its multicast forwarding table as a group-member interface.

Table entries for interfaces that the switch learns about are subject to aging. For example, if a learned multicast-router interface does not receive IGMP queries or PIM hellos within a certain interval, the switch removes the entry for that interface from its multicast forwarding 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. The switch adds a static interface to its multicast forwarding table without having to learn about the interface, and the entry in the table is not subject to aging. 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 21](#)
- [Scenario 2: Switch Forwarding Multicast Traffic to Another Switch on page 22](#)
- [Scenario 3: Switch Connected to Hosts Only \(No IGMP Querier\) on page 23](#)
- [Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs on page 24](#)

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

In the topology shown in [Figure 2 on page 22](#), a switch acting as a 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.

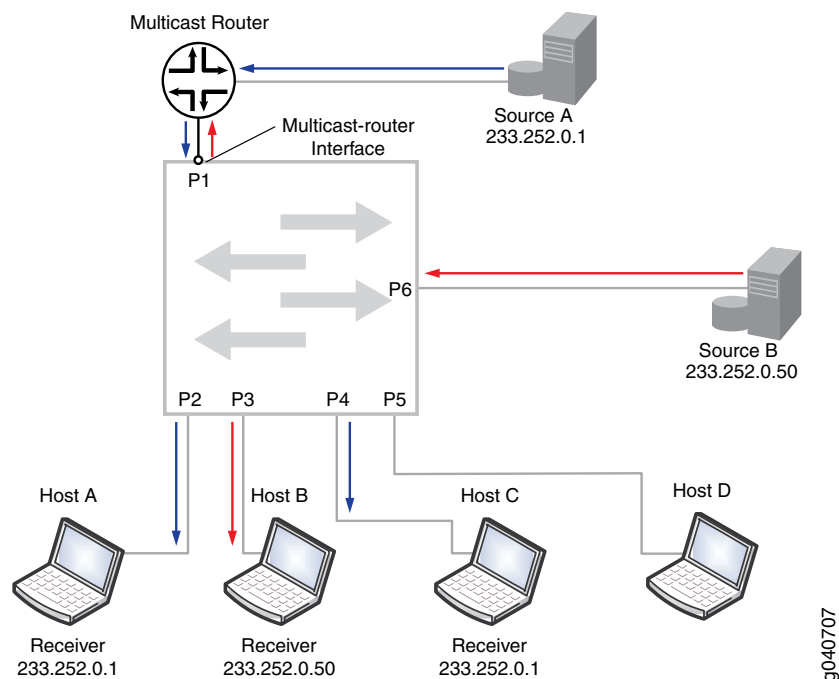
Because the switch receives IGMP queries from the multicast router on interface P1, IGMP snooping learns that interface P1 is a multicast-router interface and adds the interface to its multicast cache table. It forwards any IGMP general queries it receives on this

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



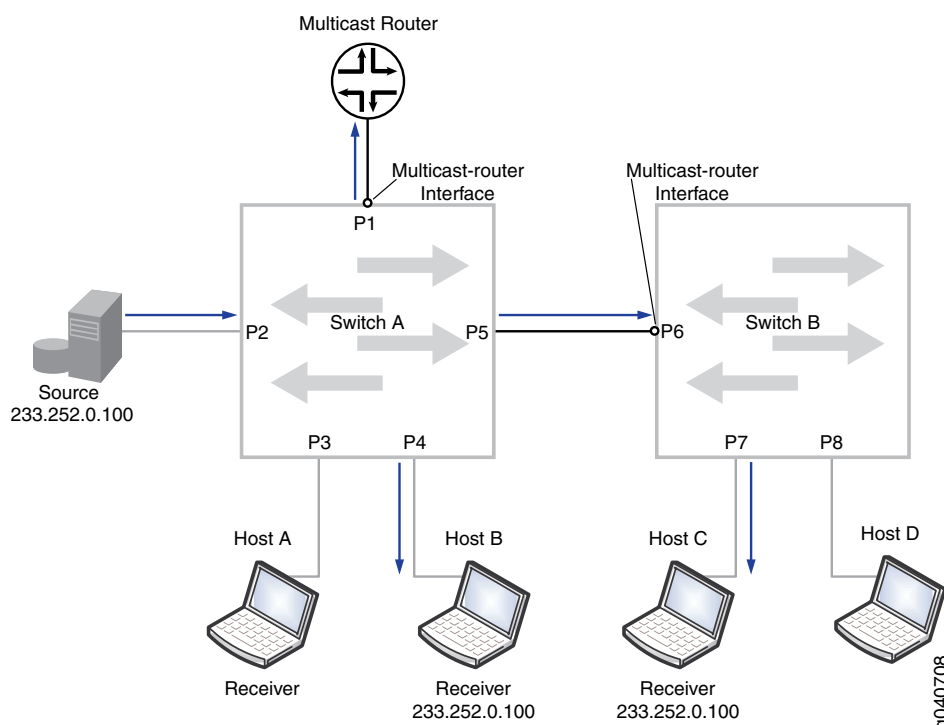
Scenario 2: Switch Forwarding Multicast Traffic to Another Switch

In the topology shown in [Figure 3 on page 23](#), 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 3: Scenario 2: Switch Forwarding Multicast Traffic to Another Switch



In certain implementations, you might have to configure P6 on Switch B as a static multicast-router interface to avoid a delay in a host receiving multicast traffic. For example, if Switch B receives unsolicited membership reports from its hosts before it learns which interface is its multicast-router interface, it does not forward those reports to Switch A. If Switch A then receives multicast traffic, it does not forward the traffic to Switch B, because it has not received any membership reports on interface P5. This issue will resolve when the multicast router sends out its next general query; however, it can cause a delay in the host receiving multicast traffic. You can statically configure interface P6 as a multicast-router interface to solve this issue.

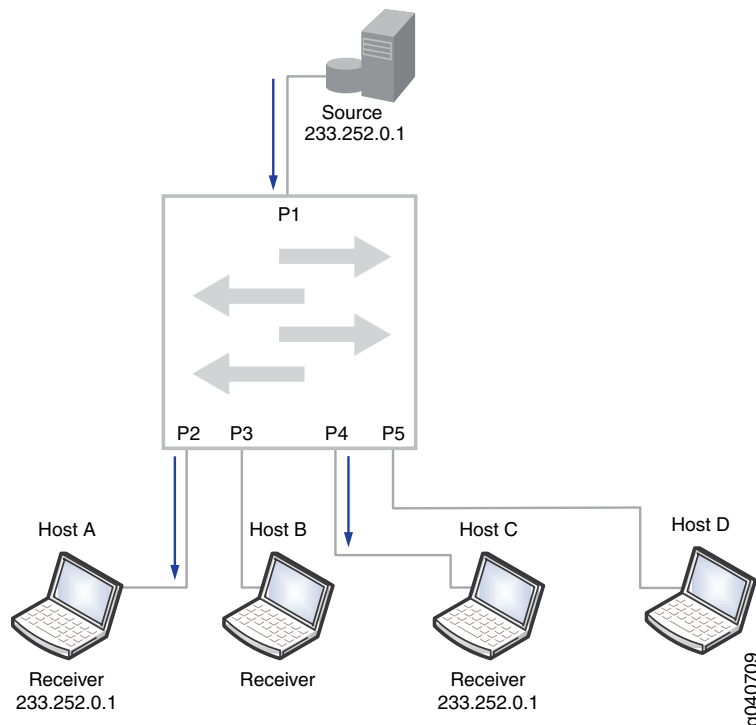
Scenario 3: Switch Connected to Hosts Only (No IGMP Querier)

In the topology shown in [Figure 4 on page 24](#), 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 4: Scenario 3: Switch Connected to Hosts Only (No IGMP Querier)

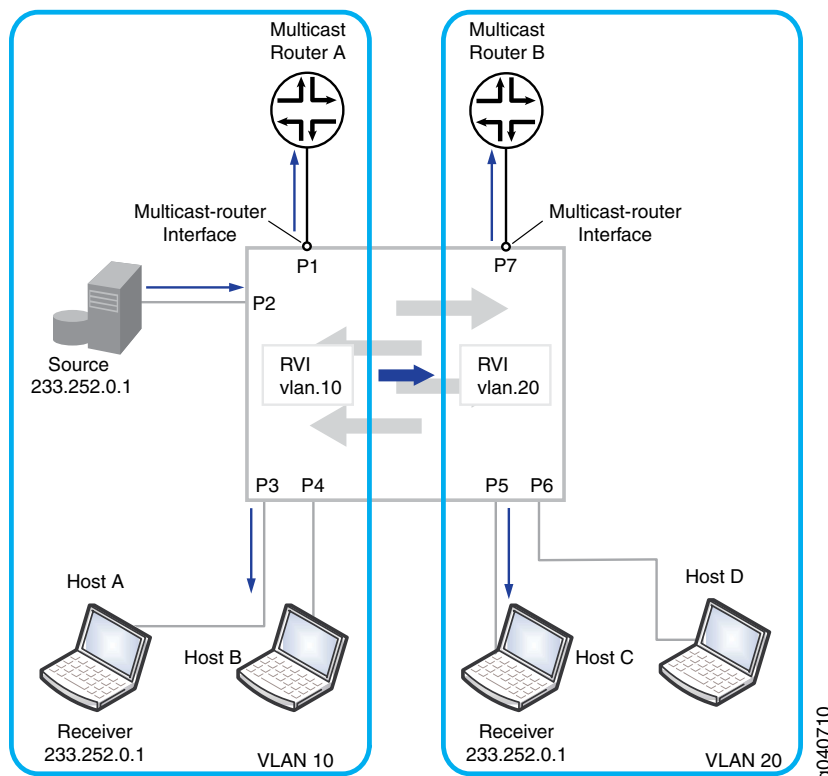


Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs

In the topology shown in [Figure 5 on page 25](#), 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 5: Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs



Related Documentation

- *Understanding Multicast VLAN Registration*
- *Example: Configuring IGMP Snooping on EX Series Switches*
- *Configuring IGMP Snooping (CLI Procedure)*
- *Configuring Routed VLAN Interfaces (CLI Procedure)*

Configuring IGMP Snooping (CLI Procedure)



NOTE: This topic uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see: *Configuring IGMP Snooping*. For ELS details see, *Getting Started with Enhanced Layer 2 Software*.

Internet Group Management Protocol (IGMP) snooping constrains the flooding of IPv4 multicast traffic on a VLAN. When IGMP snooping is enabled, a switch examines IGMP messages between hosts and multicast routers and learns which hosts are interested in receiving multicast traffic for a multicast group. Based on what it learns, the switch then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding the traffic to all interfaces. In IGMPv2, only one host on a interface sends a membership report in response to a group-specific query—any other interested

hosts suppress their reports to avoid a flood of reports for the same group. This report-suppression feature means that the switch only knows about only one interested host at any given time.

By default, IGMP snooping is enabled on the default VLAN. For many networks, IGMP snooping requires no further configuration.

You can perform the following optional configurations for each VLAN:

- Selectively enable IGMP snooping on specific VLANs.
- Enable immediate leave on a VLAN or all VLANs. Enabling immediate leave ensures that the switch stops forwarding multicast traffic immediately after the last member host on the interface leaves the group.
- Configure an interface as a static multicast-router interface for a VLAN so that the switch does not need to dynamically learn that the interface is a multicast-router interface.
- Configure an interface as a static member of a multicast group so that the switch does not need to dynamically learn the interface's membership.
- Change the value for certain timers and counters to match the values configured on the multicast router serving as the IGMP querier.

This topic covers:

- [Enabling IGMP Snooping on VLANs on page 26](#)
- [Enabling Immediate Leave on page 26](#)
- [Configuring an Interface as a Multicast-Router Interface on page 27](#)
- [Configuring Static Group Membership on an Interface on page 28](#)
- [Changing the Timer and Counter Values on page 29](#)

Enabling IGMP Snooping on VLANs

This topic describes how you can selectively enable IGMP snooping on VLANs. It assumes that you are beginning with the factory default configuration.

- To enable IGMP snooping on a VLAN:

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

You can also deactivate the IGMP snooping protocol on the switch without changing the IGMP snooping VLAN configurations:

```
[edit]  
user@switch# deactivate protocols igmp-snooping
```

Enabling Immediate Leave

By default, when a switch with IGMP snooping enabled receives an IGMP leave report on a member interface, it waits for hosts on the interface to respond to IGMP group-specific queries to determine whether there still are hosts on the interface interested

in receiving the group multicast traffic. If the switch does not see any membership reports for the group within a set interval of time, it removes the interface's group membership from the multicast forwarding table and stops forwarding multicast traffic for the group to the interface.

You can decrease the leave latency created by this default behavior by enabling immediate leave on a VLAN.

When you enable immediate leave on a VLAN, host tracking is also enabled, which allows the switch to keep track of the hosts on an interface that have joined a multicast group. When the switch receives a leave report from the last member of the group, it immediately stops forwarding traffic to the interface and does not wait for the interface group membership to time out.

Immediate leave is supported for both IGMP version 2 (IGMPv2) and IGMPv3. However, with IGMPv2, we recommend that you configure immediate leave only when there is only one IGMP host on an interface.

To enable immediate leave on a VLAN:

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

Configuring an Interface as a Multicast-Router Interface

When IGMP snooping is enabled on a switch, the switch determines which interfaces face a multicast router by monitoring interfaces for IGMP queries. If the switch receives these messages on an interface, it adds the interface to its multicast forwarding table as a multicast-router interface.

In addition to dynamically learned interfaces, the multicast forwarding table can include interfaces that you explicitly configure to be multicast-router interfaces. Unlike the table entries for dynamically learned interfaces, table entries for statically configured interfaces are not subject to aging and deletion from the forwarding table.

Examples of when you might want to configure a static multicast-router interface include:

- You have an unusual network configuration that prevents IGMP snooping from reliably learning about a multicast-router interface through monitoring IGMP queries.
- Your implementation does not require an IGMP querier.
- You have a stable topology and want to avoid the delay the dynamic learning process entails.



NOTE: All unregistered multicast packets, whether they are IPv4 or IPv6 packets, are forwarded only to the multicast-router interface.

To configure an interface as a static multicast-router interface:

```
[edit protocols]
```

```
user@switch# set igmp-snooping vlan vlan-name interface interface-name
multicast-router-interface
```

For example, to configure ge-0/0/5.0 as a multicast-router interface on a VLAN vlan100 on the switch:

```
[edit protocols]
user@switch# set igmp-snooping vlan vlan100 interface ge-0/0/5.0
multicast-router-interface
```

Configuring Static Group Membership on an Interface

To determine how to forward multicast packets, a switch with IGMP snooping enabled maintains a multicast forwarding table containing a list of host interfaces that have interested listeners for a specific multicast group. The switch learns which host interfaces to add or delete from this table by examining IGMP membership reports as they arrive on interfaces on which IGMP snooping is enabled.

In addition to such dynamically learned interfaces, the multicast forwarding table can include interfaces that you statically configure to be members of multicast groups. When you configure a static group interface, the switch adds the interface to the forwarding table as a host interface for the group. Unlike an entry for a dynamically learned interface, a static interface entry is not subject to aging and deletion from the forwarding table.

Examples of when you might want to configure static group membership on an interface include:

- You want to simulate an attached multicast receiver for testing purposes.
- The interface has receivers that cannot send IGMP membership reports.
- You want the multicast traffic for a specific group to be immediately available to a receiver without any delay imposed by the dynamic join process.



NOTE: The switch does not simulate IGMP membership reports on behalf of a statically configured interface. Thus a multicast router might be unaware that the switch has an interface that is a member of the multicast group. You can configure a static group interface on the router to ensure that the switch receives the group multicast traffic.

To configure a host interface as a static member of a multicast group:

```
[edit protocols]
user@switch# set igmp-snooping vlan vlan-name interface interface-name static group
ip-address
```

For example, to configure interface ge-0/0/11.0 in vlan100 as a static member of multicast group 225.0.0.1:

```
[edit protocols]
user@switch# set igmp-snooping vlan vlan100 interface ge-0/0/11.0 static group
225.0.0.1
```

Changing the Timer and Counter Values

IGMP uses various timers and counters to determine how often an IGMP querier sends out membership queries and when group memberships time out. On EX Series switches, the default values of the IGMP and IGMP snooping timers and counters are set to the values recommended in RFC 2236, *Internet Group Management Protocol, Version 2*. These values work well for most multicast implementations.

There might be cases, however, where you might want to modify the timer and counter values—for example, to reduce burstiness, to reduce leave latency, or to adjust for expected packet loss on a subnet. If you change a timer or counter value for the IGMP querier on a VLAN, we recommend that you change the value for all multicast routers and switches on the VLAN so that all devices time out group memberships at approximately the same time.

You can configure the following timers and counters on a switch:

- **query-interval**—The length of time the IGMP querier waits between sending general queries (the default is 125 seconds). You can change this interval to tune the number of IGMP messages on the subnet; larger values cause general queries to be sent less often.

You cannot configure this value directly for IGMP snooping. IGMP snooping inherits the value from the IGMP value configured on the switch, which is applied to all VLANs on the switch.

To configure the IGMP **query-interval**:

```
[edit protocols]
user@switch# set igmp-snooping vlan
vlan-name query-interval seconds
```

- **query-response-interval**—The maximum length of time the host can wait until it responds (the default is 10 seconds). You can change this interval to adjust the burst peaks of IGMP messages on the subnet. Set a larger interval to make the traffic less bursty.

You cannot configure this value directly for IGMP snooping. IGMP snooping inherits the value from the IGMP value configured on the switch, which is applied to all VLANs on the switch.

To configure the IGMP **query-response-interval**:

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

query-response-interval seconds
```

- **query-last-member-interval**—The length of time the IGMP querier waits between sending group-specific membership queries (the default is 1 second). The IGMP querier sends a group-specific query after receiving a leave report from a host. You can decrease this interval to reduce the amount of time it takes for multicast traffic to stop forwarding traffic after the last member leaves a group.

You cannot configure this value directly for IGMP snooping. IGMP snooping inherits the value from the IGMP value configured on the switch, which is applied to all VLANs on the switch.

To configure the IGMP **query-last-member-interval**:

[edit protocols]

```
user@switch# set igmp-snooping vlan vlan-name query-last-member-interval seconds
```

- **robust-count**—The number of times the querier resends a general membership query or a group-specific membership query (the default is 2 times). You can increase this count to tune for higher expected packet loss.

For IGMP snooping, you can configure **robust-count** for a specific VLAN. If a VLAN does not have **robust-count** configured, the robust-count value is the value configured for IGMP.

To configure robust-count for IGMP snooping on a VLAN:

[edit protocols]

```
user@switch# set igmp-snooping vlan vlan-name robust-count number
```

The values configured for **query-interval**, **query-response-interval**, and **robust-count** determine the multicast listener interval—the length of time the switch waits for a group membership report after a general query before removing a multicast group from its multicast forwarding table. The switch calculates the multicast listener interval by multiplying **query-interval** by the **robust-count** and then adding **query-response-interval** to the product:

$(\text{query-interval} * \text{robust-count}) + \text{query-response-interval} = \text{multicast listener interval}$.

For example, the multicast listener interval is 260 seconds when the default settings for **query-interval**, **query-response-interval**, and **robust-count** are used:

$(125 * 2) + 10 = 260$

You can display the time remaining in the multicast listener interval before a group times out by using the **show igmp-snooping membership** command.

Related Documentation

- [Example: Configuring IGMP Snooping on page 32](#)
- [Verifying IGMP Snooping \(CLI Procedure\) on page 38](#)
- [IGMP Snooping on EX Series Switches Overview on page 17](#)

Configuring IGMP Snooping (J-Web Procedure)



NOTE: This topic applies only to the J-Web Application package.

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 by using the J-Web interface:

1. Select **Configure > Switching > IGMP Snooping**.



NOTE: After you make changes to the configuration on 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 of the following options:

- **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 31](#).

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**.



NOTE: The **Disable** option is not available for EX4300 switches.

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 (IGMP version 2 and IGMP version 3 only).	To enable the option, select the check box. To disable the option, clear the check box.
Robust Count	Specifies the number of timeout intervals the switch waits before timing out a multicast group.	Type a value.

Table 3: IGMP Snooping Configuration Fields (*continued*)

Field	Function	Your Action
Interfaces List	Statically configures an interface as a switching interface toward a multicast router or as a member of a multicast group.	<p>Click one of the following options:</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. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the 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](#)
 - [Configuring IGMP Snooping \(CLI Procedure\)](#)
 - [IGMP Snooping on EX Series Switches Overview on page 17](#)

Example: Configuring IGMP Snooping



NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see, *Example: Configuring IGMP Snooping on EX Series Switches*. For ELS details, see, *Getting Started with Enhanced Layer 2 Software*.

You can enable IGMP snooping on a VLAN to constrain the flooding of IPv4 multicast traffic on a VLAN. When IGMP snooping is enabled, a switch examines IGMP messages between hosts and multicast routers and learns which hosts are interested in receiving multicast traffic for a multicast group. Based on what it learns, the switch then forwards multicast traffic only to those interfaces that are connected to relevant receivers instead of flooding the traffic to all interfaces.

This example describes how to configure IGMP snooping:

- [Requirements on page 33](#)
- [Overview and Topology on page 33](#)
- [Configuration on page 35](#)
- [Verifying IGMP Snooping Operation on page 35](#)

Requirements

This example uses the following hardware and software components:

- One EX4300 Series switch
- Junos OS Release 13.2X50-D10 or later for EX Series switches

Before you configure IGMP snooping, be sure you have:

- Configured a VLAN, vlan100, on the switch
- Assigned interfaces ge-0/0/0, ge-0/0/1, ge-0/0/2, and ge-0/0/12 to vlan100
- Configured ge-0/0/12 as a trunk interface

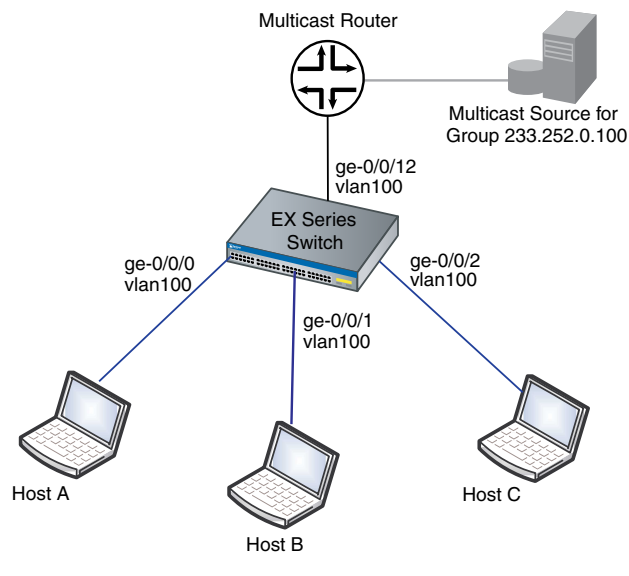
See *Configuring VLANs for EX Series Switches (CLI Procedure)*.

Overview and Topology

In this example, interfaces ge-0/0/0, ge-0/0/1, and ge-0/0/2 on the switch are in vlan100 and are connected to hosts that are potential multicast receivers. Interface ge-0/0/12, a trunk interface also in vlan100, is connected to a multicast router. The router acts as the IGMP querier and forwards multicast traffic for group 225.100.100.100 to the switch from a multicast source.

The sample topology is illustrated in [Figure 6 on page 34](#).

Figure 6: IGMP Snooping Topology Sample Topology



In this sample topology, the multicast router forwards multicast traffic to the switch from the source when it receives a membership report for group 255.100.100.100 from one of the hosts—for example, Host B. If IGMP snooping is not enabled on vlan100, the switch floods the multicast traffic on all interfaces in vlan100 (except for interface ge-0/0/12). If IGMP snooping is enabled on vlan100, the switch monitors the IGMP messages between the hosts and router, allowing it to determine that only Host B is interested in receiving the multicast traffic. The switch then forwards the multicast traffic only to interface ge-0/0/1.

This example shows how to perform the following optional configurations, which can reduce group join and leave latency:

- Configure immediate leave on the VLAN. When immediate leave is configured, the switch stops forwarding multicast traffic on an interface when it detects that the last member of the multicast group has left the group. If immediate leave is not configured, the switch waits until the group-specific queries time out before it stops forwarding traffic.

Immediate leave is supported by IGMP version 2 (IGMPv2) and IGMPv3. With IGMPv2, we recommend that you configure immediate leave only when there is only one IGMP host on an interface. In IGMPv2, only one host on a interface sends a membership report in response to a group-specific query—any other interested hosts suppress their reports to avoid a flood of reports for the same group. This report-suppression feature implies that the switch knows about only one interested host at any given time.

- Configure ge-0/0/12 as a static multicast-router interface. In this topology, ge-0/0/12 always leads to the multicast router. By statically configuring ge-0/0/12 as a multicast-router interface, you avoid any delay imposed by the switch having to learn that ge-0/0/12 is a multicast-router interface.

Configuration

To configure 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]
set protocols igmp-snooping vlan vlan100 immediate-leave
set protocols igmp-snooping vlan vlan100 interface ge-0/0/12 multicast-router-interface
```

Step-by-Step Procedure

To configure IGMP snooping on vlan100:

1. Configure the switch to immediately remove a group membership from an interface when it receives a leave report from the last member of the group on the interface:

```
[edit protocols]
user@switch# set igmp-snooping vlan vlan100 immediate-leave
```

2. Statically configure interface ge-0/0/12 as a multicast-router interface:

```
[edit protocols]
user@switch# set igmp-snooping vlan vlan100 interface ge-0/0/12
multicast-router-interface
```

Results

Check the results of the configuration:

```
[edit protocols]
user@switch# show igmp-snooping
vlan vlan100 {
    immediate-leave;
    interface ge-0/0/12.0 {
        multicast-router-interface;
    }
}
```

Verifying IGMP Snooping Operation

To verify that IGMP snooping is operating as configured, perform the following task:

- [Displaying IGMP Snooping Information for VLAN vlan100 on page 35](#)

Displaying IGMP Snooping Information for VLAN vlan100

Purpose

Verify that IGMP snooping is enabled on vlan100 and that ge-0/0/12 is recognized as a multicast-router interface.

Action

Enter the following command:

```
user@switch>show igmp snooping membership
VLAN: vlan100
Interfaces: ge-0/0/12.0,
```

Meaning

By showing information for vlan100, the command output confirms that IGMP snooping is configured on the VLAN. Interface ge-0/0/12.0 is listed as a multicast-router interface, as configured. Because none of the host interfaces are listed, none of the hosts are currently receivers for the multicast group.

- Related Documentation**
- [Configuring IGMP Snooping \(CLI Procedure\)](#)
 - [Verifying IGMP Snooping \(CLI Procedure\) on page 38](#)
 - [IGMP Snooping on EX Series Switches Overview on page 17](#)

Configuring IGMP Snooping Tracing Operations (CLI Procedure)

By enabling tracing operations for IGMP snooping, you can record detailed messages about the operation of the protocol, such as the various types of protocol packets sent and received. [Table 4 on page 36](#) describes the tracing operations you can enable and the flags used to specify them in the tracing configuration.

Table 4: Supported Tracing Operations for IGMP Snooping

Tracing Operation	Flag
Trace all (equivalent of including all flags).	all
Trace general IGMP snooping protocol events.	general
Trace communication over routing socket events.	krt
Trace leave reports (IGMPv2 and IGMPv3 only).	leave
Trace nexthop-related events.	nexthop
Trace normal IGMP snooping protocol events. If you do not specify this flag, only unusual or abnormal operations are traced.	normal
Trace all IGMP packets.	packets
Trace policy processing.	policy
Trace IGMP membership query messages.	query
Trace membership reports	report
Trace routing information.	route
Trace state transitions.	state
Trace routing protocol task processing.	task
Trace timer processing.	timer
Trace VLAN-related events.	vlan

This topic covers:

- [Configuring Tracing Operations on page 37](#)
- [Viewing, Stopping, and Restarting Tracing Operations on page 37](#)

Configuring Tracing Operations

To configure tracing operations for IGMP snooping:

1. Configure the filename for the trace file:

```
[edit protocols igmp-snooping ]
user@switch# set traceoptions file filename
```

For example:

```
[edit protocols igmp-snooping ]
user@switch# set traceoptions file mld-snoop-trace
```

2. (Optional) Configure the maximum number of trace files and size of the trace files:

```
[edit protocols igmp-snooping ]
user@switch # set file files number size size
```

For example:

```
[edit protocols igmp-snooping ]
user@switch # set traceoptions file files 5 size 1m
```

causes the contents of the trace file to be emptied and archived in a .gz file when the file reaches 1 MB. Four archive files are maintained, the contents of which are rotated whenever the current active trace file is archived.

If you omit this step, the maximum number of trace files defaults to 10, with the maximum file size defaulting to 128 K.

3. Specify one of the tracing flags shown in [Table 4 on page 36](#):

```
[edit protocols igmp-snooping ]
user@switch # set traceoptions flag flagname
```

For example, to perform trace operations on VLAN-related events and IGMP query messages:

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

[edit protocols igmp-snooping ]
user@switch# set traceoptions flag query
```

Viewing, Stopping, and Restarting Tracing Operations

When you commit the configuration, tracing operations begin. You can view the trace file in the `/var/log` directory. For example:

```
user@switch> file show /var/log/igmp-snoop-trace
```

You can stop and restart tracing operations by deactivating and reactivating the configuration:

```
[edit]
user@switch# deactivate protocols igmp-snooping traceoptions
```

```
[edit]
user@switch# activate protocols igmp-snooping traceoptions
```

- Related Documentation**
- *Configuring IGMP Snooping (CLI Procedure)*
 - *Tracing and Logging Junos OS Operations*

Verifying IGMP Snooping (CLI Procedure)

Internet Group Management Protocol (IGMP) snooping constrains the flooding of IPv4 multicast traffic on VLANs on a switch. This topic describes how to verify IGMP snooping operation on the switch.

It covers:

- [Verifying IGMP Snooping Memberships on page 38](#)
- [Viewing IGMP Snooping Statistics on page 39](#)
- [Viewing IGMP Snooping Routing Information on page 39](#)

Verifying IGMP Snooping Memberships

Purpose Determine group memberships, multicast-router interfaces, host IGMP versions, and the current values of timeout counters.

Action Enter the following command:

```
user@switch> show igmp-snooping membership detail
VLAN: vlan2 Tag: 2 (Index: 3)
  Router interfaces:
    ge-1/0/0.0 dynamic Uptime: 00:14:24 timeout: 253
  Group: 225.0.0.1
    ge-1/0/17.0 259 Last reporter: 13.0.0.90 Receiver count: 1
    Uptime: 00:00:19 timeout: 259 Flags: <V3-hosts>
    Include source: 10.2.11.5, 10.2.11.12
```

Meaning The switch has multicast membership information for one VLAN on the switch, **vlan2**. IGMP snooping might be enabled on other VLANs, but the switch does not have any multicast membership information for them. The following information is provided:

- Information on the multicast-router interfaces for the VLAN—in this case, **ge-1/0/0.0**. The multicast-router interface has been learned by IGMP snooping, as indicated by the dynamic value. The timeout value shows how many seconds from now the interface will be removed from the multicast forwarding table if the switch does not receive IGMP queries or Protocol Independent Multicast (PIM) updates on the interface.
- Information about the group memberships for the VLAN:

- Currently, the VLAN has membership in only one multicast group, **225.0.0.1**.
- The host or hosts that have reported membership in the group are on interface **ge-1/0/17.0**. The last host that reported membership in the group has address **13.0.0.90**. The number of hosts belonging to the group on the interface is shown in the Receiver count field, which is displayed only when host tracking is enabled if immediate leave is configured on the VLAN.
- The Uptime field shows that the multicast group has been active on the interface for 19 seconds. The interface group membership will time out in 259 seconds if no hosts respond to membership queries during this interval. The Flags field shows the lowest version of IGMP used by a host that is currently a member of the group, which in this case is IGMP version 3 (IGMPv3).
- Because the interface has IGMPv3 hosts on it, the source addresses from which the IGMPv3 hosts want to receive group multicast traffic are shown (addresses **10.2.11.5** and **10.2.11.12**). The timeout value for the interface group membership is derived from the largest timeout value for all sources addresses for the group.

Viewing IGMP Snooping Statistics

Purpose Display IGMP snooping statistics, such as number of IGMP queries, reports, and leaves received and how many of these IGMP messages contained errors.

Action Enter the following command:

```
user@switch> show igmp-snooping statistics
```

```
Bad length: 0 Bad checksum: 0 Invalid interface: 0
Not local: 0 Receive unknown: 0 Timed out: 0
```

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

Meaning The output shows how many IGMP messages of each type—**Queries**, **Reports**, **Leaves**—the switch received or transmitted on interfaces on which IGMP snooping is enabled. For each message type, it also shows the number of IGMP packets the switch received that had errors—for example, packets that do not conform to the IGMPv1, IGMPv2, or IGMPv3 standards. If the **Recv Errors** count increases, verify that the hosts are compliant with IGMP standards. If the switch is unable to recognize the IGMP message type for a packet, it counts the packet under **Receive unknown**.

Viewing IGMP Snooping Routing Information

Purpose Display the next-hop information maintained in the multicast forwarding table.

Action Enter the following command:

```
user@switch> show igmp-snooping route detail
```

```
VLAN      Group      Next-hop
v100      224.0.0.0, * 1323
```

```

          Interfaces: ge-0/0/0.0
VLAN      Group      Next-hop
v100      226.0.0.1, * 1322
          Interfaces: ge-0/0/0.0, ge-0/0/1.0, ge-0/0/47.0

```

Meaning The output shows the next-hop interfaces for a given multicast group on a VLAN. For example, route 226.0.0.1 on v100 has next-hop interfaces **ge-0/0/0.0**, **ge-0/0/1.0**, and **ge-0/0/47.0**.

Related Documentation

- [clear igmp-snooping membership on page 136](#)
- [clear igmp-snooping statistics on page 137](#)
- *Example: Configuring IGMP Snooping on EX Series Switches*
- *Configuring IGMP Snooping (CLI Procedure)*

Monitoring IGMP Snooping

Purpose



NOTE: This topic applies only to the J-Web Application package.

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 route**
- **show igmp-snooping statistics**
- **show igmp-snooping vlans**



NOTE: On EX4300 switches, to display IGMP snooping details in the CLI, enter the following commands:

- **show igmp snooping interface**
- **show igmp snooping statistics**
- **show multicast snooping next-hops**
- **show multicast snooping route**

Meaning [Table 5 on page 41](#) summarizes the IGMP snooping details displayed.

Table 5: 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.
Learning Domain	Learning domain for snooping.
NOTE: This option is supported only on EX4300 switches.	
Query Interval	Frequency (in seconds) with which the router sends membership queries when it is the querier.
NOTE: This option is supported only on EX4300 switches.	
Query Response Interval	Time (in seconds) that the router waits for a response to a general query.
NOTE: This option is supported only on EX4300 switches.	
Last Member Query Interval	Time (in seconds) that the router waits for a report in response to a group-specific query.
NOTE: This option is supported only on EX4300 switches.	
Robustness Count	Number of times the router retries a query.
NOTE: This option is supported only on EX4300 switches.	
MRouters	Specifies the multicast router.
NOTE: This option is not supported on EX4300 switches.	
Receivers	Specifies the multicast receiver.
NOTE: This option is not supported on EX4300 switches.	
Interface Details	
Interfaces	Name of the interface.
NOTE: This option is only supported on EX4300 switches.	
State	Operating state of the interface. Values are Up or Down.
NOTE: This option is only supported on EX4300 switches.	
Group count	Number of groups on the interface.
NOTE: This option is only supported on EX4300 switches.	

Table 5: Summary of IGMP Snooping Output Fields (*continued*)

Field	Values
Immediate Leave NOTE: This option is only supported on EX4300 switches.	State of immediate leave. Values are On or Off.
Router Interface NOTE: This option is only supported on EX4300 switches.	Router interfaces that are part of this learning domain.
IGMP Route Information	
VLAN NOTE: This option is not supported on EX4300 switches.	The VLAN for which IGMP snooping is enabled.
Group NOTE: This option is not supported on EX4300 switches.	Indicates the multicast groups learned by the VLAN.
Next-Hop NOTE: This option is not supported on EX4300 switches.	Specifies the next hop assigned by the switch after performing the route lookup.
Statistics	
Packets per Vlan NOTE: This option is supported only on EX4300 switches.	Displays the number of packets sent or received, or the number of received errors.
Global NOTE: This option is supported only on EX4300 switches.	Displays the statistics name and statistics count. The statistics names are: <ul style="list-style-type: none"> • Bad Length • Bad Checksum • Bad Receive If • Rx non-local • Timed out
Multicast Snooping Nexthops	
ID NOTE: This option is supported only on EX4300 switches.	Next-hop identifier of the prefix. The identifier is returned by the routing device's Packet Forwarding Engine.
Reference Count NOTE: This option is supported only on EX4300 switches.	Number of cache entries that are using this next hop.
Kernel Reference Count NOTE: This option is supported only on EX4300 switches.	Kernel reference count for the next hop.

Table 5: Summary of IGMP Snooping Output Fields (*continued*)

Field	Values
Downstream Interface	Interface names associated with each multicast next-hop ID.
NOTE: This option is supported only on EX4300 switches.	

- Related Documentation
- [show igmp-snooping route on page 175](#)
 - [show igmp-snooping statistics on page 177](#)
 - *show igmp-snooping vlans*
 - *Configuring IGMP Snooping (CLI Procedure)*
 - *Example: Configuring IGMP Snooping on EX Series Switches*

CHAPTER 2

Configuration Statements

- [\[edit protocols\] Configuration Statement Hierarchy on EX Series Switches on page 47](#)
- [\[edit protocols igmp-snooping\] Configuration Statement Hierarchy on page 48](#)
- [accounting \(Protocols IGMP Interface\) on page 50](#)
- [accounting \(Protocols IGMP\) on page 50](#)
- [address \(Anycast RPs\) on page 51](#)
- [address \(Local RPs\) on page 52](#)
- [anycast-pim on page 53](#)
- [assert-timeout on page 54](#)
- [auto-rp on page 55](#)
- [bootstrap on page 56](#)
- [bootstrap-export on page 57](#)
- [bootstrap-import on page 58](#)
- [bootstrap-priority on page 59](#)
- [data-forwarding on page 60](#)
- [dense-groups on page 61](#)
- [disable \(IGMP Snooping\) on page 61](#)
- [disable \(Protocols IGMP\) on page 62](#)
- [disable \(PIM\) on page 63](#)
- [dr-election-on-p2p on page 64](#)
- [dr-register-policy on page 64](#)
- [embedded-rp on page 65](#)
- [export \(Bootstrap\) on page 66](#)
- [family \(Bootstrap\) on page 67](#)
- [family \(Local RP\) on page 68](#)
- [graceful-restart \(Protocols PIM\) on page 69](#)
- [group \(IGMP Snooping\) on page 69](#)
- [group \(Protocols IGMP\) on page 70](#)
- [group-ranges on page 71](#)

- [hello-interval](#) on page 72
- [hold-time \(Protocols PIM\)](#) on page 73
- [igmp-snooping](#) on page 74
- [immediate-leave \(Protocols IGMP\)](#) on page 75
- [immediate-leave \(IGMP Snooping\)](#) on page 76
- [import \(Protocols PIM Bootstrap\)](#) on page 77
- [import \(Protocols PIM\)](#) on page 78
- [infinity](#) on page 79
- [interface \(IGMP Snooping\)](#) on page 80
- [interface \(Protocols PIM\)](#) on page 81
- [interface \(Protocols IGMP\)](#) on page 83
- [join-load-balance](#) on page 84
- [local](#) on page 85
- [local-address \(Protocols PIM\)](#) on page 86
- [mapping-agent-election](#) on page 87
- [maximum-rps](#) on page 88
- [mode \(Protocols PIM\)](#) on page 89
- [multicast-router-interface \(IGMP Snooping\)](#) on page 90
- [neighbor-policy](#) on page 91
- [pim](#) on page 92
- [priority \(PIM Interfaces\)](#) on page 96
- [priority \(Bootstrap\)](#) on page 97
- [priority \(PIM RPs\)](#) on page 98
- [query-interval \(Protocols IGMP\)](#) on page 99
- [query-last-member-interval \(Protocols IGMP\)](#) on page 100
- [query-response-interval \(Protocols IGMP\)](#) on page 101
- [receiver](#) on page 102
- [register-probe-time](#) on page 102
- [restart-duration \(Protocols PIM\)](#) on page 103
- [rib-group \(Protocols PIM\)](#) on page 104
- [robust-count \(IGMP Snooping\)](#) on page 105
- [robust-count \(Protocols IGMP\)](#) on page 105
- [rp](#) on page 106
- [rp-register-policy](#) on page 108
- [rp-set](#) on page 109
- [source \(Protocols IGMP\)](#) on page 110
- [source-vlans](#) on page 111

- [spt-threshold](#) on page 112
- [ssm-map \(Protocols IGMP\)](#) on page 113
- [static \(IGMP Snooping\)](#) on page 113
- [static \(Protocols PIM\)](#) on page 114
- [static \(Protocols IGMP\)](#) on page 115
- [traceoptions \(Protocols PIM\)](#) on page 116
- [traceoptions \(Protocols IGMP\)](#) on page 119
- [traceoptions \(IGMP Snooping\)](#) on page 122
- [version \(Protocols IGMP\)](#) on page 124
- [version \(IGMP Snooping\)](#) on page 125
- [version \(PIM\)](#) on page 126
- [vlan \(IGMP Snooping\)](#) on page 127

[\[edit protocols\]](#) Configuration Statement Hierarchy on EX Series Switches

Each of the following topics lists the statements at a subhierarchy of the [\[edit protocols\]](#) hierarchy:

- [\[edit protocols bfd\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols bgp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols connections\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols dcbx\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols dot1x\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols igmp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols igmp-snooping\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols isis\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols lacp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols link-management\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols lldp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols lldp-med\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols mld\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols mld-snooping\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols mpls\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols msdp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols mstp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols mvrp\]](#) Configuration Statement Hierarchy on EX Series Switches

- [\[edit protocols neighbor-discovery\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols oam\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols ospf\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols ospf3\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols pim\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols rip\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols ripng\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols router-advertisement\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols router-discovery\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols rstp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols rsvp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols sflow\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols stp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols uplink-failure-detection\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols vrrp\]](#) Configuration Statement Hierarchy on EX Series Switches
- [\[edit protocols vstp\]](#) Configuration Statement Hierarchy on EX Series Switches

**Related
Documentation**

- [EX Series Switch Software Features Overview](#)
- [EX Series Virtual Chassis Software Features Overview](#)

[\[edit protocols igmp-snooping\]](#) Configuration Statement Hierarchy

This topic lists supported and unsupported configuration statements in the [\[edit protocols igmp-snooping\]](#) hierarchy level on EX Series switches.

- *Supported* statements are those that you can use to configure some aspect of a software feature on the switch.
- *Unsupported* statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see [EX Series Switch Software Features Overview](#).

This topic lists:

- [Supported Statements in the \[edit protocols igmp-snooping\] Hierarchy Level on page 49](#)
- [Unsupported Statements in the \[edit protocols igmp-snooping\] Hierarchy Level on page 49](#)

Supported Statements in the [edit protocols igmp-snooping] Hierarchy Level

The following hierarchy shows the **[edit protocols igmp-snooping]** configuration statements supported on EX Series switches:

```
protocols {
  igmp-snooping {
    vlan vlan-name {
      immediate-leave;
      interface interface-name {
        group-limit <1..65535>
        host-only-interface
        multicast-router-interface;
        immediate-leave;
        static {
          group multicast-ip-address {
            source <>
          }
        }
      }
    }
    l2-querier {
      source-address ip-address;
    }
    proxy {
      source-address ip-address;
    }
    query-interval number;
    query-last-member-interval number;
    query-response-interval number;
    robust-count number;
    traceoptions {
      file filename <files number> <no-stamp> <replace> <size maximum-file-size>
        <world-readable | no-world-readable>;
      flag flag <flag-modifier>;
    }
  }
}
```

Unsupported Statements in the [edit protocols igmp-snooping] Hierarchy Level

All statements in the **[edit protocols igmp-snooping]** hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

Related Documentation

- [\[edit protocols\] Configuration Statement Hierarchy on EX Series Switches on page 47](#)

accounting (Protocols IGMP 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. Statement introduced in Junos OS Release 12.1 for the QFX Series.
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">• <i>Recording IGMP Join and Leave Events</i>

accounting (Protocols IGMP)

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. Statement introduced in Junos OS Release 12.1 for the QFX Series.
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">• <i>Recording IGMP Join and Leave Events</i>

address (Anycast RPs)

Syntax	<code>address <i>address</i> <forward-msdp-sa>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols <code>pim rp local</code> (inet inet6) <code>anycast-pim rp-set</code>],</p> <p>[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>],</p> <p>[edit protocols <code>pim rp local</code> (inet inet6) <code>anycast-pim rp-set</code>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols <code>pim rp local</code> (inet inet6) <code>anycast-pim rp-set</code>]</p>
Release Information	<p>Statement introduced in Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p>
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	<p><i>address</i>—RP address in an RP set.</p> <p><i>forward-msdp-sa</i>—(Optional) Forward MSDP SAs to this address.</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>

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. Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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">• <i>Configuring Local PIM RPs</i>

anycast-pim

Syntax	<pre>anycast-pim { rp-set { address address <forward-msdp-sa>; } }</pre>
Hierarchy Level	<p>[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)]</p>
Release Information	<p>Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series.</p>
Description	<p>Configure properties for anycast RP using PIM.</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	<ul style="list-style-type: none"> • <i>Example: Configuring PIM Anycast With or Without MSDP</i>

assert-timeout

Syntax	<code>assert-timeout 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. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	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.
Options	seconds —Time for routing device to wait before another assert message cycle. Range: 5 through 210 seconds Default: 180 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">• <i>Example: Configuring the PIM Assert Timeout</i>

auto-rp

Syntax	<pre> auto-rp { (announce discovery mapping); (mapping-agent-election no-mapping-agent-election); } </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 7.5.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p>
Description	Configure automatic RP announcement and discovery.
Options	<p>announce—Configure the routing device to listen only for mapping packets and also to advertise itself if it is an RP.</p> <p>discovery—Configure the routing device to listen only for mapping packets.</p> <p>mapping—Configures the routing device to announce, listen for and generate mapping packets, and announce that the routing device is eligible to be an RP.</p> <p>The remaining statement is 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"> • <i>Configuring PIM Auto-RP</i>

bootstrap

Syntax	<pre>bootstrap { family (inet inet6) { export [<i>policy-names</i>]; import [<i>policy-names</i>]; priority <i>number</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 in Junos OS Release 7.6. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	Configure parameters to control bootstrap routers and messages. 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">• <i>Configuring PIM Bootstrap Properties for IPv4</i>• <i>Configuring PIM Bootstrap Properties for IPv4 or IPv6</i>

bootstrap-export

Syntax	<code>bootstrap-export [<i>policy-names</i>];</code>
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>Statement introduced in Junos OS Release 11.3 for the QFX Series.</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"> • <i>Configuring PIM Bootstrap Properties for IPv4</i> • <i>Configuring PIM Bootstrap Properties for IPv4 or IPv6</i> • bootstrap-import on page 58

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. Statement introduced in Junos OS Release 11.3 for the QFX Series.
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">• <i>Configuring PIM Bootstrap Properties for IPv4</i>• <i>Configuring PIM Bootstrap Properties for IPv4 or IPv6</i>• bootstrap-export on page 57

bootstrap-priority

Syntax	<code>bootstrap-priority <i>number</i>;</code>
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>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p>
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	<p><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.</p> <p>Range: 0 through 255</p> <p>Default: 0</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"> • <i>Configuring PIM Bootstrap Properties for IPv4</i>

data-forwarding

Syntax	<pre>data-forwarding { receiver { source-vlans <i>vlan-list</i>; install; } source { groups <i>group-prefix</i>; } }</pre>
Hierarchy Level	[edit protocols igmp-snooping vlan (all <i>vlan-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.6 for EX Series switches. Statement introduced in Junos OS Release 12.3 for the QFX Series.
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 IGMP version 2 (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">• <i>Example: Configuring Multicast VLAN Registration</i>• <i>Configuring Multicast VLAN Registration (CLI Procedure)</i>

dense-groups

Syntax	<code>dense-groups { addresses; }</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. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	Configure which groups are operating in dense mode.
Options	addresses —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"> • <i>Configuring PIM Sparse-Dense Mode Properties</i>

disable (IGMP Snooping)

Syntax	<code>disable;</code>
Hierarchy Level	[edit protocols igmp-snooping vlan (all <i>vlan-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.2 for EX Series switches.
Description	Disable IGMP snooping on the VLAN. Multicast traffic will be flooded to all interfaces on the VLAN except the source interface.
Default	If you do not include this statement in the configuration for a VLAN, IGMP snooping is enabled on the VLAN.
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"> • <i>Configuring IGMP Snooping (CLI Procedure)</i> • <i>show igmp-snooping vlans</i>

disable (Protocols IGMP)

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. Statement introduced in Junos OS Release 12.1 for the QFX Series.
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">• <i>Disabling IGMP</i>

disable (PIM)

Syntax	disable;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim family (inet inet6)],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp local family (inet inet6)],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp local family (inet inet6)],</p> <p>[edit protocols pim],</p> <p>[edit protocols pim family (inet inet6)],</p> <p>[edit protocols pim interface <i>interface-name</i>],</p> <p>[edit protocols pim rp local family (inet inet6)],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim family (inet inet6)],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i>],</p> <p>[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> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</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 PIM family (Protocols PIM)

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. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	Enable PIM designated router (DR) election on point-to-point (P2P) links.
Default	No PIM DR election is performed on point-to-point 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">• <i>Configuring PIM Designated Router Election on Point-to-Point Links</i>

dr-register-policy

Syntax	dr-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. Statement introduced in Junos OS Release 11.3 for the QFX Series.
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">• <i>Configuring Register Message Filters on a PIM RP and DR</i>• rp-register-policy on page 108

embedded-rp

Syntax	<pre> embedded-rp { group-ranges { destination-ip-prefix </prefix-length>; } maximum-rps limit; } </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>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p>
Description	<p>Configure properties for embedded IP version 6 (IPv6) RPs.</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"> • <i>Configuring PIM Embedded RP for IPv6</i>

export (Bootstrap)

Syntax	<code>export [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp bootstrap family (inet inet6)], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap family (inet inet6)], [edit protocols pim rp bootstrap family (inet inet6)], [edit routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap family (inet inet6)]
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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">• <i>Configuring PIM Bootstrap Properties for IPv4</i>• <i>Configuring PIM Bootstrap Properties for IPv4 or IPv6</i>• import (Protocols PIM Bootstrap) on page 77

family (Bootstrap)

Syntax	<pre>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 bootstrap],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap],</p> <p>[edit protocols pim rp bootstrap],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap]</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> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p>
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	<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"> • <i>Configuring PIM Bootstrap Properties for IPv4</i> • <i>Configuring PIM Bootstrap Properties for IPv4 or IPv6</i>

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; override; priority number; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp local], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp local], [edit protocols pim rp local], [edit routing-instances <i>routing-instance-name</i> protocols pim rp local]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	Configure which IP protocol type local RP properties to apply.
Options	inet —Apply IP version 4 (IPv4) local RP properties. inet6 —Apply IPv6 local RP properties. 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"><i>Configuring Local PIM RPs</i>


graceful-restart (Protocols PIM)

Syntax	graceful-restart { disable; no-bidirectional-mode; restart-duration seconds; }
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. Statement introduced in Junos OS Release 11.3 for the QFX Series.
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 (IGMP Snooping)

Syntax	group <i>ip-address</i> ;
Hierarchy Level	[edit protocols igmp-snooping <i>vlan</i> (all <i>vlan-name</i>) interface (all <i>interface-name</i>) static]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Configure a static multicast group on an interface.
Options	<i>ip-address</i> —Valid IP multicast address for the multicast group.
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 IGMP Snooping (CLI Procedure) • show igmp-snooping membership on page 172

group (Protocols IGMP)

Syntax	<pre>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>; } }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i> static], [edit protocols igmp interface <i>interface-name</i> static]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 12.1 for the QFX Series.
Description	Specify the IGMP multicast group address and (optionally) the source address for the multicast group being statically configured on an interface.
<hr/> <div> NOTE: You must specify a unique address for each group.</div> <hr/>	
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">• <i>Enabling IGMP Static Group Membership</i>

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 bidirectional address <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp embedded-rp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols pim rp bidirectional address <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp embedded-rp],</p> <p>[edit protocols pim rp bidirectional address <i>address</i>],</p> <p>[edit protocols pim rp embedded-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>instance-name</i> protocols pim rp bidirectional address <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp embedded-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> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> <p>Support for bidirectional RP addresses introduced in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 13.3 for the PTX5000 router.</p>
Description	Configure the address ranges of the multicast groups for which this routing device can be a rendezvous point (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-ip-prefix</prefix-length></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"> • <i>Configuring Local PIM RPs</i> • <i>Configuring PIM Embedded RP for IPv6</i> • <i>Example: Configuring Bidirectional PIM</i>

hello-interval

Syntax	<code>hello-interval seconds;</code>
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. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	Specify how often the routing device 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 (Protocols PIM) on page 73• <i>Modifying the PIM Hello Interval</i>


hold-time (Protocols PIM)

Syntax	<code>hold-time seconds;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp bidirectional address <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols pim rp bidirectional address <i>address</i>],</p> <p>[edit protocols pim rp bidirectional address <i>address</i>],</p> <p>[edit protocols pim rp local family (inet inet6)],</p> <p>[edit routing-instances <i>instance-name</i> protocols pim rp bidirectional address <i>address</i>],</p> <p>[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>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Support for bidirectional RP addresses introduced in Junos OS Release 12.1.</p>
Description	Specify the time period for which a neighbor is to consider the sending routing device (this routing device) to be operative (up).
Options	<p>seconds—Hold time.</p> <p>Range: 1 through 255</p> <p>Default: 150 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"> • <i>Configuring Local PIM RPs</i> • <i>Example: Configuring Bidirectional PIM</i>


igmp-snooping

Syntax	<pre> igmp-snooping { traceoptions { file <i>filename</i> <files <i>number</i>> <no-stamp> <replace> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i> <<i>flag-modifier</i>>; } vlan (all <i>vlan-name</i>) { } immediate-leave; interface (all <i>interface-name</i>) { group-limit <i>range</i>; host-only-interface; multicast-router-interface; immediate-leave; static { group <i>multicast-ip-address</i>; } } l2-querier { source-address <i>ip-address</i>; } proxy { source-address <i>ip-address</i>; } query-interval <i>number</i>; query-last-member-interval <i>number</i>; query-response-interval <i>number</i>; robust-count <i>number</i>; version <i>version</i>; } </pre>
Hierarchy Level	[edit protocols]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	<p>Configure IGMP snooping. The factory default configuration enables IGMP snooping on all VLANs.</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"> Example: Configuring IGMP Snooping on EX Series Switches Configuring IGMP Snooping (CLI Procedure)

immediate-leave (Protocols IGMP)

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. Statement introduced in Junos OS Release 12.1 for the QFX Series.
Description	<p>The immediate leave setting is useful for minimizing the leave latency of IGMP memberships. When this setting is enabled, the routing device leaves the multicast group immediately after the last host leaves the multicast group.</p> <p>The immediate leave setting enables host tracking, meaning that the device keeps track of the hosts that send join messages. This allows IGMP to determine when the last host sends a leave message for the multicast group.</p> <p>When the immediate leave setting is enabled, the device removes an interface from the forwarding-table entry without first sending IGMP group-specific queries to the interface. The interface is pruned from the multicast tree for the multicast group specified in the IGMP leave message. The immediate leave setting ensures optimal bandwidth management for hosts on a switched network, even when multiple multicast groups are being used simultaneously.</p> <p>When immediate leave is disabled and one host sends a leave group message, the routing device first sends a group query to determine if another receiver responds. If no receiver responds, the routing device removes all hosts on the interface from the multicast group. Immediate leave is disabled by default for both IGMP version 2 and IGMP version 3.</p>
	<p> NOTE: Although host tracking is enabled for IGMPv2 and MLDv1 when you enable immediate leave, use immediate leave with these versions only when there is one host on the interface. The reason is that IGMPv2 and MLDv1 use a report suppression mechanism whereby only one host on an interface sends a group join report in response to a membership query. The other interested hosts suppress their reports. The purpose of this mechanism is to avoid a flood of reports for the same group. But it also interferes with host tracking, because the router only knows about the one interested host and does not know about the others.</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"> <i>Specifying Immediate-Leave Host Removal for IGMP</i>

immediate-leave (IGMP Snooping)

Syntax	immediate-leave;
Hierarchy Level	[edit protocols igmp-snooping vlan (all <i>vlan-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	<p>Configure IGMP snooping immediate leave for the specified VLAN. When you configure immediate leave, host tracking is enabled, which allows the switch to track the hosts that send membership reports. The switch can then determine when the last host on an interface leaves the multicast group and immediately stop forwarding multicast traffic to the interface.</p> <p>Configuring immediate leave reduces the amount of time it takes for the switch to stop sending multicast traffic to an interface when the last host leaves the group. When immediate leave is disabled, the switch no longer tracks hosts. Instead, whenever it receives a leave report from a host, it sends out a group-specific query to all hosts. If it does not receive any membership reports on the interface in response to the group-specific query within a set interval, it stops forwarding multicast traffic to the interface.</p>
	<div> NOTE: Immediate leave is supported for both IGMP version 2 (IGMPv2) and IGMPv3. However, with IGMPv2, we recommend that you configure immediate leave only when there is only one IGMP host on an interface. In IGMPv2, only one host on a interface sends a membership report in response to a general query—any other interested hosts suppress their reports. Report suppression avoids a flood of reports for the same group, but it also interferes with host tracking because the switch knows only about one interested host on the interface at any given time.</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">• <i>Example: Configuring IGMP Snooping on EX Series Switches</i>• <i>Configuring IGMP Snooping (CLI Procedure)</i>

import (Protocols PIM Bootstrap)

Syntax	<code>import [<i>policy-names</i>];</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp bootstrap (inet inet6)],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap (inet inet6)],</p> <p>[edit protocols pim rp bootstrap (inet inet6)],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap (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> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
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	<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"> • <i>Configuring PIM Bootstrap Properties for IPv4</i> • <i>Configuring PIM Bootstrap Properties for IPv4 or IPv6</i> • export (Bootstrap) on page 66

import (Protocols 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. Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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 and prevent them 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">• <i>Filtering Incoming PIM Join Messages</i>

infinity

Syntax	<code>infinity [<i>policy-names</i>];</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim spt-threshold],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim spt-threshold],</p> <p>[edit protocols pim spt-threshold],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim spt-threshold]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.0.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p>
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	<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"> • <i>Example: Configuring the PIM SPT Threshold Policy</i>

interface (IGMP Snooping)

Syntax	<pre>interface <i>interface-name</i> { multicast-router-interface; static { group <i>ip-address</i>; } }</pre>
Hierarchy Level	[edit protocols igmp-snooping vlan (all <i>vlan-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	For IGMP snooping, configure an interface as either a multicast-router interface or as a static member of a multicast group.
Options	<p>all—All interfaces in the VLAN.</p> <p><i>interface-name</i>—Name of the interface.</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">• <i>Example: Configuring IGMP Snooping on EX Series Switches</i>• <i>Configuring IGMP Snooping (CLI Procedure)</i>• <i>show igmp-snooping vlans</i>

interface (Protocols PIM)

```
Syntax interface (Protocols PIM) (all | 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;
        no-adaptation;
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        version (0 | 1 | automatic);
    }
    bidirectional {
        df-election {
            backoff-period milliseconds;
            offer-period milliseconds;
            robustness-count number;
        }
    }
    family (inet | inet6) {
        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;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (0 | 1 | automatic);
        }
        disable;
    }
    hello-interval seconds;
}
```

```
mode (bidirectional-sparse | bidirectional-sparse-dense | dense | sparse | sparse-dense);
neighbor-policy [ policy-names ];
override-interval milliseconds;
priority number;
propagation-delay milliseconds;
reset-tracking-bit;
version version;
}
```

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 Enable PIM on an interface and configure interface-specific properties.

Options *interface-name*—Name of the interface. Specify the full interface name, including the
physical and logical address components. To configure all interfaces, you can specify
[all](#).

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

- [PIM on Aggregated Interfaces](#)

interface (Protocols IGMP)

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>; ssm-map-policy <i>ssm-map-policy-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. Statement introduced in Junos OS Release 12.1 for the QFX Series.
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"> • <i>Enabling IGMP</i>

join-load-balance

Syntax	<pre>join-load-balance { automatic; }</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 in Junos OS Release 9.0. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	Enable load balancing of PIM join messages across interfaces and routing devices.
Options	automatic —Enables automatic load balancing of PIM join messages. When a new interface or neighbor is introduced into the network, ECMP joins are redistributed with minimal disruption to traffic.
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">• <i>Configuring PIM Join Load Balancing</i>• <i>clear pim join-distribution</i> in the CLI Explorer

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; override; priority number; } group-ranges { destination-ip-prefix</prefix-length>; } hold-time seconds; override; 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>Statement introduced in Junos OS Release 11.3 for the QFX Series.</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"> <i>Configuring Local PIM RPs</i>

local-address (Protocols PIM)

Syntax	<code>local-address address;</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> protocols pim rp local family (inet inet6) anycast-pim],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp local family (inet inet6) anycast-pim],</code> <code>[edit protocols pim rp local family (inet inet6) anycast-pim],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols pim rp local family (inet inet6) anycast-pim]</code>
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	Configure the routing device local address for the anycast rendezvous point (RP). If this statement is omitted, the router ID is used as this address.
Options	address —Anycast RP IPv4 or IPv6 address, depending on family configuration.
Required Privilege Level	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring PIM Anycast With or Without MSDP</i>

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. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	Configure the routing device 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"> • <i>Configuring PIM Auto-RP</i>


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. Statement introduced in Junos OS Release 11.3 for the QFX Series.
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">• <i>Configuring PIM Embedded RP for IPv6</i>

mode (Protocols PIM)

Syntax	mode (bidirectional-sparse bidirectional-sparse-dense dense sparse sparse-dense);
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. bidirectional-sparse and bidirectional-sparse-dense options introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 13.3 for the PTX5000 router.
Description	Configure the PIM mode on the interface.
Options	<p>The choice of PIM mode is closely tied to controlling how groups are mapped to PIM modes, as follows:</p> <ul style="list-style-type: none"> • bidirectional-sparse—Use if all multicast groups are operating in bidirectional, sparse, or SSM mode. • bidirectional-sparse-dense—Use if multicast groups, except those that are specified in the dense-groups statement, are operating in bidirectional, sparse, or SSM mode. • dense—Use if all multicast groups are operating in dense mode. • sparse—Use if all multicast groups are operating in sparse mode or SSM mode. • sparse-dense—Use if multicast groups, except those that are specified in the dense-groups statement, are operating in sparse mode or SSM mode. <p>Default: Sparse mode</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"> • <i>Configuring PIM Dense Mode Properties in the Multicast Protocols Feature Guide for Routing Devices</i> • <i>Configuring PIM Sparse-Dense Mode Properties in the Multicast Protocols Feature Guide for Routing Devices</i> • <i>Example: Configuring Bidirectional PIM</i>

multicast-router-interface (IGMP Snooping)

Syntax	multicast-router-interface;
Hierarchy Level	<p>[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface <i>interface-name</i>],</p> <p>[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping vlan <i>vlan-id</i> interface <i>interface-name</i>],</p> <p>[edit protocols igmp-snooping vlan (all <i>vlan-name</i>) interface (all <i>interface-name</i>)],</p> <p>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols vlan <i>vlan-id</i> igmp-snooping interface <i>interface-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.5.</p> <p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p>
Description	<p>Statically configure the interface as an IGMP snooping multicast-router interface—that is, an interface that faces toward a multicast router or other IGMP querier.</p>
	<p> NOTE: If the specified interface is a trunk port, the interface becomes a multicast-routing device interface for all VLANs configured on the trunk port. In addition, all unregistered multicast packets, whether they are IPv4 or IPv6 packets, are forwarded to the multicast routing device interface, even if the interface is configured as a multicast routing device interface only for IGMP snooping.</p> <p>Configure an interface as a bridge interface toward other multicast routing devices.</p>
Default	The interface can either be a host-side or multicast-routing device interface.
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"> • <i>Example: Configuring IGMP Snooping</i> • <i>IGMP Snooping in MC-LAG Active-Active Mode</i> • <i>host-only-interface</i>

neighbor-policy

Syntax	<code>neighbor-policy [<i>policy-names</i>];</code>
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 in Junos OS Release 8.2. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series.
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"> • <i>Configuring Interface-Level PIM Neighbor Policies</i>

pim

```
Syntax  pim {
    disable;
    assert-timeout seconds;
    dense-groups {
        addresses;
    }
    dr-election-on-p2p;
    export ;
    family (inet | inet6) {
        disable;
    }
    graceful-restart {
        disable;
        no-bidirectional-mode;
        restart-duration seconds;
    }
    import [ policy-names ];
    interface interface-name {
        family (inet | inet6) {
            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;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (0 | 1 | automatic);
        }
        accept-remote-source;
        disable;
        bidirectional {
            df-election {
                backoff-period milliseconds;
                offer-period milliseconds;
                robustness-count number;
            }
        }
        family (inet | inet6) {
            disable;
        }
        hello-interval seconds;
    }
}
```

```

mode (bidirectional-sparse | bidirectional-sparse-dense | 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;
mdt {
  data-mdt-reuse;
  group-range multicast-prefix;
  threshold {
    group group-address {
      source source-address {
        rate threshold-rate;
      }
    }
  }
  tunnel-limit limit;
}
}
mvpn {
  autodiscovery {
    inet-mdt;
  }
}
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);
  }
  bidirectional {
    address address {
      group-ranges {
        destination-ip-prefix</prefix-length>;
      }
      hold-time seconds;
      priority number;
    }
  }
  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;  
}  
group-rp-mapping {  
    family (inet | inet6) {  
        log-interval seconds;  
        maximum limit;  
        threshold value;  
    }  
}  
log-interval seconds;  
maximum limit;  
threshold value;  
}  
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;  
        override;  
        priority number;  
    }  
}  
register-limit {  
    family (inet | inet6) {  
        log-interval seconds;  
        maximum limit;  
        threshold value;  
    }  
}  
log-interval seconds;  
maximum limit;  
threshold value;  
}  
rp-register-policy [ policy-names ];  
spt-threshold {  
    infinity [ policy-names ];  
}  
static {  
    address address {
```

```

        override;
        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;
        }
    }
}
sglimit {
    family (inet | inet6) {
        log-interval seconds;
        maximum limit;
        threshold value;
    }
    log-interval seconds;
    maximum limit;
    threshold value;
}
}
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 *logical-system-name* protocols],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols],
 [edit protocols],
 [edit routing-instances *routing-instance-name* 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 remaining 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">• <i>Example: Configuring Data MDTs and Provider Tunnels Operating in Any-Source Multicast Mode</i>• <i>Configuring PIM Dense Mode Properties</i>• <i>Configuring PIM Sparse-Dense Mode Properties</i>

priority (PIM Interfaces)

Syntax	<code>priority number;</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 before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the routing device's likelihood to be elected as the designated router.
Options	number —Routing device's priority for becoming the designated router. A higher value corresponds to a higher priority. Range: 0 through 4294967295 Default: 1 (Each routing device has an equal probability of becoming the DR.)
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">• <i>Configuring Interface Priority for PIM Designated Router Selection</i>

priority (Bootstrap)

Syntax	<code>priority <i>number</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp bootstrap (inet inet6)],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap (inet inet6)],</p> <p>[edit protocols pim rp bootstrap (inet inet6)],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap (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> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Configure the routing device's likelihood to be elected as the bootstrap router.
Options	<p><i>number</i>—Routing device's priority for becoming the bootstrap router. A higher value corresponds to a higher priority.</p> <p>Range: 0 through a 32-bit number</p> <p>Default: 0 (The routing device has the least likelihood of becoming the bootstrap router and sends packets with a priority of 0.)</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"> • <i>Configuring PIM Bootstrap Properties for IPv4</i> • <i>Configuring PIM Bootstrap Properties for IPv4 or IPv6</i> • bootstrap-priority on page 59

priority (PIM RPs)

Syntax	<code>priority <i>number</i>;</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> protocols pim rp bidirectional address <i>address</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols pim</code> <code>rp bidirectional address <i>address</i>],</code> <code>[edit protocols pim rp bidirectional address <i>address</i>],</code> <code>[edit protocols pim rp local family (inet inet6)],</code> <code>[edit routing-instances <i>instance-name</i> protocols pim rp bidirectional address <i>address</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols pim rp local family (inet inet6)]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series. Support for bidirectional RP addresses introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 13.3 for the PTX5000 router.
Description	For PIM-SM, configure this routing device's priority for becoming an RP. For bidirectional PIM, configure this RP address' priority for becoming an RP. The bootstrap router uses this field when selecting the list of candidate rendezvous points to send in the bootstrap message. A smaller number increases the likelihood that the routing device or RP address becomes the RP. A priority value of 0 means that bootstrap router can override the group range being advertised by the candidate RP.
Options	<i>number</i> —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">• <i>Configuring Local PIM RPs</i>• <i>Example: Configuring Bidirectional PIM</i>

query-interval (Protocols IGMP)

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. Statement introduced in Junos OS Release 12.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify how often the querier routing device 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"> • <i>Modifying the IGMP Host-Query Message Interval</i> • query-last-member-interval (Protocols IGMP) on page 100 • query-response-interval (Protocols IGMP) on page 101

query-last-member-interval (Protocols IGMP)

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. Statement introduced in Junos OS Release 12.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify how often the querier routing device 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 9999999 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">• <i>Modifying the IGMP Last-Member Query Interval</i>• query-interval (Protocols IGMP) on page 99• query-response-interval (Protocols IGMP) on page 101

query-response-interval (Protocols IGMP)

Syntax	query-response-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. Statement introduced in Junos OS Release 12.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify how long the querier routing device waits to receive a response to a host-query message from a host.
Options	seconds —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">• <i>Modifying the IGMP Query Response Interval</i>• query-interval (Protocols IGMP) on page 99• query-last-member-interval (Protocols IGMP) on page 100

receiver

Syntax	<pre>receiver { source-vlans <i>vlan-list</i>; install; }</pre>
Hierarchy Level	[edit protocols igmp-snooping vlan (all <i>vlan-name</i>) data-forwarding]
Release Information	Statement introduced in Junos OS Release 9.6 for EX Series switches. Statement introduced in Junos OS Release 12.3 for the QFX Series.
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">• <i>Example: Configuring Multicast VLAN Registration</i>• <i>Configuring Multicast VLAN Registration (CLI Procedure)</i>

register-probe-time

Syntax	<pre>register-probe-time <i>register-probe-time</i>;</pre>
Hierarchy Level	[edit protocols pim rp]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D16 for QFX Series switches.
Description	Specify the amount of time before the register suppression time (RST) expires when a designated switch can send a NULL-Register to the rendezvous point (RP).
Options	<i>register-probe-time</i> —Amount of time before the RST expires. Default: 5 seconds Range: 5 to 60 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">• <i>PIM Overview</i>• <i>Understanding PIM Sparse Mode</i>

restart-duration (Protocols PIM)

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. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	Configure the duration of the graceful restart interval.
Options	<i>seconds</i> —Time that 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"> <i>Configuring PIM Sparse Mode Graceful Restart</i>

rib-group (Protocols PIM)

Syntax	<pre>rib-group { inet <i>group-name</i>; inet6 <i>group-name</i>; }</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. Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Associate a routing table group with PIM.
Options	<i>table-name</i> —Name of the routing table. The name must be one that you defined with the rib-groups 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">• <i>Example: Configuring a Dedicated PIM RPF Routing Table</i>

robust-count (IGMP Snooping)

Syntax	<code>robust-count <i>number</i>;</code>
Hierarchy Level	[edit protocols igmp-snooping vlan (all <i>vlan-name</i>)]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Configure the number of queries the switch sends before removing a multicast group from the multicast forwarding table. We recommend that the robust count be set to the same value on all multicast routers and switches in the VLAN.
Default	The default is the value of the robust-count statement configured for IGMP. The default for the IGMP robust-count statement is 2.
Options	<i>number</i> —Number of queries the switch sends 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"> • <i>Configuring IGMP Snooping (CLI Procedure)</i>

robust-count (Protocols IGMP)

Syntax	<code>robust-count <i>number</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. Statement introduced in Junos OS Release 12.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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"> • <i>Modifying the IGMP Robustness Variable</i>

rp

```

Syntax  register-probe-time {
        auto-rp {
            (announce | discovery | mapping);
            (mapping-agent-election | no-mapping-agent-election);
        }
        bidirectional {
            address address {
                group-ranges {
                    destination-ip-prefix </prefix-length>;
                }
                hold-time seconds;
                priority number;
            }
        }
        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;
        }
        group-rp-mapping {
            family (inet | inet6) {
                log-interval seconds;
                maximum limit;
                threshold value;
            }
        }
        log-interval seconds;
        maximum limit;
        threshold value;
    }
    local {
        family (inet | inet6) {
            disable;
            address address;
            anycast-pim {
                local-address address;
                address address <forward-msdp-sa>;
                rp-set {
            }
        }
    }

```

```

    }
    group-ranges {
        destination-ip-prefix</prefix-length>;
    }
    hold-time seconds;
    override;
    priority number;
}
}
register-limit {
    family (inet | inet6) {
        log-interval seconds;
        maximum limit;
        threshold value;
    }
}
log-interval seconds;
maximum limit;
threshold value;
}
}
register-probe-time register-probe-time;
}
rp-register-policy [ policy-names ];
static {
    address address {
        override;
        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.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

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

- *Understanding PIM Sparse Mode*

rp-register-policy

Syntax `rp-register-policy [policy-names];`

Hierarchy Level [edit logical-systems *logical-system-name* protocols [pim rp](#)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols [pim rp](#)],
[edit protocols [pim rp](#)],
[edit routing-instances *routing-instance-name* 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.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Apply one or more policies to control incoming PIM register messages.

Options *policy-names*—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

- *Configuring Register Message Filters on a PIM RP and DR*
- [dr-register-policy on page 64](#)

rp-set

Syntax	<pre>rp-set { address address <forward-msdp-sa>; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim local family (inet inet6) anycast-pim],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim local family (inet inet6) anycast-pim],</p> <p>[edit protocols pim local family (inet inet6) anycast-pim],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim local family (inet inet6) anycast-pim]</p>
Release Information	<p>Statement introduced in Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Configure a set of rendezvous point (RP) addresses for anycast RP. You can configure up to 15 RPs.</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"> • <i>Example: Configuring PIM Anycast With or Without MSDP</i>

source (Protocols IGMP)

Syntax	<code>source <i>ip-address</i> { source-count <i>number</i>; source-increment <i>increment</i>; }</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i> static group <i>multicast-group-address</i>], [edit protocols igmp interface <i>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. Statement introduced in Junos OS Release 12.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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">• <i>Enabling IGMP Static Group Membership</i>

source-vlans

Syntax	<code>source-vlans <i>vlan-list</i>;</code>
Hierarchy Level	[edit protocols igmp-snooping vlan (all <i>vlan-name</i>) data-forwarding receiver]
Release Information	Statement introduced in Junos OS Release 9.6 for EX Series switches. Statement introduced in Junos OS Release 12.3 for the QFX Series.
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">• <i>Example: Configuring Multicast VLAN Registration</i>• <i>Configuring Multicast VLAN Registration (CLI Procedure)</i>

spt-threshold

Syntax	<pre>spt-threshold { infinity [policy-names]; }</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 in Junos OS Release 8.0. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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">• <i>Example: Configuring the PIM SPT Threshold Policy</i>

ssm-map (Protocols IGMP)

Syntax	<code>ssm-map <i>ssm-map-name</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface interface-name], [edit protocols igmp interface interface-name]
Release Information	Statement introduced in Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 12.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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"> • <i>Example: Configuring SSM Mapping</i>

static (IGMP Snooping)

Syntax	<code>static { group ip-address; }</code>
Hierarchy Level	[edit protocols igmp-snooping vlan (all <i>vlan-name</i>) interface interface-name
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"> • <i>Configuring IGMP Snooping (CLI Procedure)</i> • show igmp-snooping membership on page 172

static (Protocols PIM)

Syntax	<pre>static { address address { group-ranges { destination-ip-prefix</prefix-length>; } override; version version; } }</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. Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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	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 the Static PIM RP Address on the Non-RP Routing Device

static (Protocols IGMP)

Syntax

```
static {
  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*],
[edit protocols igmp **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.
Statement introduced in Junos OS Release 12.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Test multicast forwarding on an interface without a receiver host.

The **static** statement simulates IGMP joins on a routing device statically on an interface without any IGMP hosts. It is supported for both IGMPv2 and IGMPv3 joins. This statement is especially useful for testing multicast forwarding on an interface without a receiver host.



NOTE: To prevent joining too many groups accidentally, the **static** statement is not supported with the **interface all** statement.

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

- *Enabling IGMP Static Group Membership*

traceoptions (Protocols PIM)

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. Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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• bidirectional-df-election—Bidirectional PIM designated-forwarder (DF) election events

- **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	• <i>Configuring PIM Trace Options</i>
	• <i>Tracing DVMRP Protocol Traffic</i>
	• <i>Tracing MSDP Protocol Traffic</i>
	• <i>Configuring PIM Trace Options</i>

traceoptions (Protocols IGMP)

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	<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>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
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	routing and trace—To view this statement in the configuration.
Level	routing-control and trace-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Tracing IGMP Protocol Traffic</i>

traceoptions (IGMP Snooping)

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <no-stamp> <replace> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i> <flag-modifier>; }</pre>
Hierarchy Level	[edit protocols igmp-snooping]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches. Statement introduced in Junos OS Release 13.2 for the QFX series.
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, including the active trace file. When a trace file reaches its maximum size, its contents are archived into a compressed file named <i>filename.0</i> and the trace file is emptied. When the trace file reaches its maximum size again, the <i>filename.0</i> archive file is renamed <i>filename.1</i> and a new <i>filename.0</i> archive file is created from the contents of the trace file. This process continues until the maximum number of trace files is reached, at which point the system starts overwriting the oldest archive file each time the trace file is archived. 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: 10 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.• krt—Trace communication over routing socket.• leave—Trace leave group messages (IGMPv2 and IGMPv3 only).• nexthop—Trace nexthop-related events.• normal—Trace normal IGMP snooping protocol events. If you do not specify this flag, only unusual or abnormal operations are traced.• 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.
- **vlan**—Trace VLAN-related events.

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

- **detail**—Provide detailed trace information
- **disable**—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.
- **receive**—Packets being received.
- **send**—Packets being transmitted.

no-stamp—(Optional) Omit the timestamp at the beginning of each line in the trace file.

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

replace—(Optional) Replace an existing trace file if there is one. 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 bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches its maximum size, it is zipped and 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 size, you also must specify a maximum number of files with the **files** option.

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

Range: 10240 through 4294967295 bytes

Default: 128 KB

world-readable—(Optional) Allow 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	• Configuring IGMP Snooping Tracing Operations (CLI Procedure) on page 36
------------------------------	---

version (Protocols IGMP)

Syntax	<code>version version;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface interface-name], [edit protocols igmp 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. Statement introduced in Junos OS Release 12.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the version of IGMP.
Options	version —IGMP version number. Range: 1, 2, or 3 Default: IGMP version 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">• <i>Changing the IGMP Version</i>

version (IGMP Snooping)

Syntax	<code>version number;</code>
Hierarchy Level	[edit protocols igmp-snooping vlan (all <i>vlan-name</i>)]
Release Information	Statement introduced in Junos OS Release 11.1 for EX Series switches. Statement introduced in Junos OS Release 12.1 for the QFX Series.
Description	Specify the IGMP version for the IGMP general query that the switch sends to hosts when an interface comes up. The configured IGMP version affects only the version of the general queries sent by a switch. It does not affect the version of IGMP messages that the switch can snoop. For example, If the switch is configured for IGMP version 1 (IGMPv1), it can snoop IGMPv2 and IGMPv3 messages.
Default	If you do not configure the version statement, the default is IGMPv2.
Options	version —IGMP version number. Range: 1 and 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"> • <i>Configuring IGMP Snooping (CLI Procedure)</i> • <i>Configuring IGMP Snooping</i>

version (PIM)

Syntax	<code>version version;</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> protocols <code>pim rp static address address</code>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-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 rp static address address</code>], [edit protocols <code>pim interface interface-name</code>], [edit protocols <code>pim rp static address address</code>], [edit routing-instances <i>routing-instance-name</i> protocols <code>pim interface interface-name</code>], [edit routing-instances <i>routing-instance-name</i> protocols <code>pim rp static address address</code>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the version of PIM.
Options	version —PIM version number. Range: 1 or 2 Default: PIMv1 for rendezvous point (RP) mode (at the [edit protocols <code>pim rp static address address</code>] hierarchy level). PIMv2 for interface mode (at the [edit protocols <code>pim interface interface-name</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">• <i>Enabling PIM Sparse Mode</i>• <i>Configuring PIM Dense Mode Properties</i>• <i>Configuring PIM Sparse-Dense Mode Properties</i>

vlan (IGMP Snooping)

```
Syntax  vlan (all | vlan-name) {
        data-forwarding {
            source {
                groups group-prefix;
            }
            receiver {
                source-vlans vlan-list;
                install;
            }
        }
        disable;
        immediate-leave;
        interface (all | interface-name) {
            multicast-router-interface;
            static {
                group ip-address;
            }
        }
        proxy {
            source-address ip-address;
        }
        robust-count number;
        version version;
    }
```

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.

When the **vlan** configuration statement is used without the **disable** statement, IGMP snooping is enabled on the specified VLAN or on all VLANs.



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

Default If the **vlan** statement is not included in the configuration, IGMP snooping is disabled.

- Options**
- **all**—All VLANs on the switch
 - ***vlan-name***—Name of a VLAN.



TIP: When you configure IGMP snooping parameters using the **vlan all** statement, any VLAN that is not individually configured for IGMP snooping

inherits the `vlan all` configuration. Any VLAN that is individually configured for IGMP snooping, on the other hand, inherits none of its configuration from `vlan all`. Any parameters that are not explicitly defined for the individual VLAN assume their default values, not the values specified in the `vlan all` configuration.

For example, in the following configuration:

```
protocols {
  igmp-snooping {
    vlan all {
      robust-count 8;
    }
    vlan employee {
      interface ge-0/0/8.0 {
        static {
          group 239.0.10.3
        }
      }
    }
  }
}
```

all VLANs, except `employee`, have a robust count of 8. Because `employee` has been individually configured, its robust count value is not determined by the value set under `vlan all`. Instead, its robust count is the default value of 2.

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	• <i>Example: Configuring IGMP Snooping on EX Series Switches</i>
	• <i>Configuring IGMP Snooping (CLI Procedure)</i>
	• <i>show igmp-snooping vlans</i>

CHAPTER 3

Operational Commands

- clear igmp membership
- clear igmp statistics
- clear igmp-snooping membership
- clear igmp-snooping statistics
- clear multicast bandwidth-admission
- clear multicast scope
- clear multicast sessions
- clear multicast statistics
- clear pim join
- clear pim register
- clear pim statistics
- mtrace
- mtrace from-source
- mtrace monitor
- mtrace to-gateway
- show igmp group
- show igmp interface
- show igmp statistics
- show igmp-snooping membership
- show igmp-snooping route
- show igmp-snooping statistics
- show multicast flow-map
- show multicast interface
- show multicast minfo
- show multicast next-hops
- show multicast pim-to-igmp-proxy
- show multicast pim-to-mld-proxy
- show multicast route

- `show multicast rpf`
- `show multicast scope`
- `show multicast sessions`
- `show multicast usage`
- `show pim bootstrap`
- `show pim interfaces`
- `show pim join`
- `show pim neighbors`
- `show pim rps`
- `show pim source`
- `show pim statistics`

clear igmp membership

List of Syntax	Syntax on page 131 Syntax (EX Series Switch and the QFX Series) on page 131
Syntax	<pre>clear igmp membership <group address-range> <interface interface-name> <logical-system (all logical-system-name)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>clear igmp membership <group address-range> <interface interface-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>Command introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
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 address-range—(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 interface-name—(Optional) Clear all IGMP group members on an interface.</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	clear
Related Documentation	<ul style="list-style-type: none"> • show igmp group on page 161 • show igmp interface on page 165
List of Sample Output	clear igmp membership on page 131 clear igmp membership interface on page 132 clear igmp membership group on page 133
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

List of Syntax	Syntax on page 134 Syntax (EX Series Switches) on page 134
Syntax	<code>clear igmp statistics</code> <code><interface <i>interface-name</i>></code> <code><logical-system (all <i>logical-system-name</i>)></code>
Syntax (EX Series Switches)	<code>clear igmp statistics</code> <code><interface <i>interface-name</i>></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.3 for the QFX Series.
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
List of Sample Output	clear igmp statistics on page 134
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
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
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	0		

clear igmp-snooping membership

Syntax	<code>clear igmp-snooping membership</code> <code><vlan <i>vlan-name</i>></code>
Release Information	Command introduced in Junos OS Release 9.1 for EX Series switches.
Description	Clear IGMP snooping dynamic membership information from the multicast forwarding table.
Options	none —Clear dynamic membership information for all VLANs. vlan <i>vlan-name</i> —(Optional) Clear dynamic membership information for the specified VLAN.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show igmp-snooping membership on page 172• clear igmp-snooping statistics on page 137
List of Sample Output	clear igmp-snooping membership on page 136

Sample Output

clear igmp-snooping membership

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


clear igmp-snooping statistics

Syntax	clear igmp-snooping statistics
Release Information	Command introduced in Junos 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 177• clear igmp-snooping membership on page 136
List of Sample Output	clear igmp-snooping statistics on page 137

Sample Output

clear igmp-snooping statistics

```
user@switch> clear igmp-snooping statistics
```

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	<p>Command introduced in Junos OS Release 8.3.</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> <p>Command introduced in Junos OS Release 11.3 for the QFX Series.</p>
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>group <i>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>source <i>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 • [show multicast interface on page 181](#)

List of Sample Output [clear multicast bandwidth-admission on page 139](#)

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

Sample Output

[clear multicast bandwidth-admission](#)

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

clear multicast scope

List of Syntax	Syntax on page 140 Syntax (EX Series Switch and the QFX Series) on page 140
Syntax	<pre>clear multicast scope <inet inet6> <interface <i>interface-name</i>> <logical-system (all <i>logical-system-name</i>)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>clear multicast scope <inet inet6> <interface <i>interface-name</i>></pre>
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. Command introduced in Junos OS Release 11.3 for the QFX Series.
Description	Clear IP multicast scope statistics.
Options	<p>none—(Same as logical-system all) Clear multicast scope statistics.</p> <p>inet—(Optional) Clear multicast scope statistics for IPv4 family addresses.</p> <p>inet6—(Optional) Clear multicast scope statistics for IPv6 family addresses.</p> <p>interface <i>interface-name</i>—(Optional) Clear multicast scope statistics on 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>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show multicast scope on page 202
List of Sample Output	clear multicast scope on page 140
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

List of Syntax	Syntax on page 141 Syntax (EX Series Switch and the QFX Series) on page 141
Syntax	clear multicast sessions <logical-system (all <i>logical-system-name</i>)> < <i>regular-expression</i> >
Syntax (EX Series Switch and the QFX Series)	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. Command introduced in Junos OS Release 11.3 for the QFX Series.
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 204
List of Sample Output	clear multicast sessions on page 141
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

List of Syntax	Syntax on page 142 Syntax (EX Series Switch and the QFX Series) on page 142
Syntax	<pre>clear multicast statistics <inet inet6> <instance <i>instance-name</i>> <interface <i>interface-name</i>> <logical-system (all <i>logical-system-name</i>)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>clear multicast statistics <inet inet6> <instance <i>instance-name</i>> <interface <i>interface-name</i>></pre>
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. Command introduced in Junos OS Release 11.3 for the QFX Series.
Description	Clear IP multicast statistics.
Options	<p>none—Clear multicast statistics for all supported address families on all interfaces.</p> <p>inet—(Optional) Clear multicast statistics for IPv4 family addresses.</p> <p>inet6—(Optional) Clear multicast statistics for IPv6 family addresses.</p> <p>instance <i>instance-name</i>—(Optional) Clear multicast statistics for the specified instance.</p> <p>interface <i>interface-name</i>—(Optional) Clear multicast statistics on 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>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">show multicast statistics
List of Sample Output	clear multicast statistics on page 142
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

List of Syntax	Syntax on page 143 Syntax (EX Series Switch and the QFX Series) on page 143
Syntax	<pre>clear pim join <group-address> <inet inet6> <instance instance-name> <logical-system (all logical-system-name)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>clear pim join <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> <p>Command introduced in Junos OS Release 11.3 for the QFX Series.</p>
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 215
List of Sample Output	clear pim join on page 144
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

List of Syntax	Syntax on page 145 Syntax (EX Series Switch and the QFX Series) on page 145 Syntax (PTX Series) on page 145
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 and the QFX Series)	clear pim register <inet inet6> <instance <i>instance-name</i> > <interface <i>interface-name</i> >
Syntax (PTX Series)	clear pim register <inet inet6> <instance <i>instance-name</i> > <logical-system (all <i>logical-system-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. Command introduced in Junos OS Release 11.3 for the QFX Series.
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 • [show pim statistics on page 250](#)

List of Sample Output [clear pim register on page 146](#)

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

List of Syntax	Syntax on page 147 Syntax (EX Series Switch and the QFX Series) on page 147
Syntax	<pre>clear pim statistics <inet inet6> <instance <i>instance-name</i>> <interface <i>interface-name</i>> <logical-system (all <i>logical-system-name</i>)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>clear pim statistics <inet inet6> <instance <i>instance-name</i>> <interface <i>interface-name</i>></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> <p>Command introduced in Junos OS Release 11.3 for the QFX Series.</p>
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 250
List of Sample Output	clear pim statistics on page 148
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><logical-system logical-system-name></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. Command introduced in Junos OS Release 9.5 for SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices. Command introduced in Junos OS Release 11.3 for the QFX Series. Command introduced in Junos OS Release 12.3 for the PTX Series.
Description	Display trace information about an IP multicast path.
Options	source —Source hostname or address. logical-system (logical-system-name) —(Optional) Perform this operation on a logical system. routing-instance routing-instance-name —(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 152
Output Fields	Table 6 on page 150 describes the output fields for the mtrace command. Output fields are listed in the approximate order in which they appear.

Table 6: 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.

Table 6: mtrace Output Fields (*continued*)

Field Name	Field Description
<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.

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>`
`<ttl tll>`
`<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.
 Command introduced in Junos OS Release 11.3 for the QFX Series.

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, 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 the 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 *ttl*—(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 155](#)

Output Fields [Table 7 on page 154](#) describes the output fields for the **mtrace from-source** command. Output fields are listed in the approximate order in which they appear.

Table 7: 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.
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.
source	Source address.
Response Dest	Response destination address.
Overall	Average packet rate for all traffic at each hop.

Table 7: mtrace from-source Output Fields (*continued*)

Field Name	Field Description
Packet Statistics for Traffic From	Number of packets lost, number of packets sent, percentage of packets lost, and average packet rate at each hop.
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. Command introduced in Junos OS Release 11.3 for the QFX Series.
Description	Listen passively for IP multicast responses. To exit the mtrace monitor command, type Ctrl+c.
Options	none —Trace the master instance.
Required Privilege Level	view
List of Sample Output	mtrace monitor on page 157
Output Fields	Table 8 on page 156 describes the output fields for the mtrace monitor command. Output fields are listed in the approximate order in which they appear.

Table 8: 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 2fea1d
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 <i>extra-hops</i> > <group <i>group</i> > <interface <i>interface-name</i> > <interval <i>interval</i> > <loop> <max-hops <i>max-hops</i> > <max-queries <i>max-queries</i> > <multicast-response unicast-response> <no-resolve> <no-router-alert> <response <i>response</i> > <routing-instance <i>routing-instance-name</i> > <tll <i>tll</i> > <unicast-response> <wait-time <i>wait-time</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.3 for the QFX Series.
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 <i>extra-hops</i> —(Optional) Number of hops to take after reaching a nonresponsive router or switch. You can specify a number between 0 and 255 . group <i>group</i> —(Optional) Group address for which to trace the path. The default group address is 0.0.0.0 . interface <i>interface-name</i> —(Optional) Source address for sending the trace query. interval <i>interval</i> —(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 <i>max-hops</i> —(Optional) Maximum hops to trace toward the source. You can specify a number between 0 and 255 . The default value is 32 . max-queries <i>max-queries</i> —(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 159](#)

Output Fields [Table 9 on page 159](#) describes the output fields for the **mtrace to-gateway** command. Output fields are listed in the approximate order in which they appear.

Table 9: 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.
<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.

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.lab.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

List of Syntax	Syntax on page 161 Syntax (EX Series Switch and the QFX Series) on page 161
Syntax	<pre>show igmp group <brief detail> <group-name> <logical-system (all logical-system-name)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>show igmp group <brief detail> <group-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>Command introduced in Junos OS Release 11.3 for the QFX Series.</p>
Description	Display Internet Group Management Protocol (IGMP) group membership information.
Options	<p>none—Display standard information about membership for all IGMP groups.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>group-name—(Optional) Display group membership for the specified IP address only.</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	show igmp group (Include Mode) on page 162 show igmp group (Exclude Mode) on page 163 show igmp group brief on page 163 show igmp group detail on page 163
Output Fields	<p>Table 10 on page 161 describes the output fields for the show igmp group command. Output fields are listed in the approximate order in which they appear.</p>

Table 10: 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 10: 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

List of Syntax	Syntax on page 165 Syntax (EX Series Switch and the QFX Series) on page 165
Syntax	<pre>show igmp interface <brief detail> <interface-name> <logical-system (all logical-system-name)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>show igmp interface <brief detail> <interface-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>Command introduced in Junos OS Release 11.3 for the QFX Series.</p>
Description	Display information about Internet Group Management Protocol (IGMP)-enabled interfaces.
Options	<p>none—Display standard information about all IGMP-enabled interfaces.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>interface-name—(Optional) Display information about the specified IGMP-enabled interface only.</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
Related Documentation	<ul style="list-style-type: none"> • clear igmp membership on page 131
List of Sample Output	show igmp interface on page 167 show igmp interface brief on page 167 show igmp interface detail on page 168
Output Fields	<p>Table 11 on page 165 describes the output fields for the show igmp interface command. Output fields are listed in the approximate order in which they appear.</p>

Table 11: show igmp interface Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface.	All levels
Querier	Address of the routing device that has been elected to send membership queries.	All levels

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

Field Name	Field Description	Level of Output
State	State of the interface: Up or Down .	All levels
SSM Map Policy	Name of the source-specific multicast (SSM) map policy that has been applied to the IGMP interface.	All levels
Timeout	How long until the IGMP querier is declared to be unreachable, in seconds.	All levels
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 (if configured) associated with the interface.	All levels
SSM map	Name of the source-specific multicast (SSM) map (if configured) used on the interface.	All levels

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

Field Name	Field Description	Level of Output
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
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

```

user@host> show igmp interface
Interface: at-0/3/1.0
  Querier: 10.111.30.1
  State:      Up Timeout:   None Version:  2 Groups:    4
  SSM Map Policy: ssm-policy-A
Interface: so-1/0/0.0
  Querier: 10.111.10.1
  State:      Up Timeout:   None Version:  2 Groups:    2
  SSM Map Policy: ssm-policy-B
Interface: so-1/0/1.0
  Querier: 10.111.20.1
  State:      Up Timeout:   None Version:  2 Groups:    4
  SSM Map Policy: ssm-policy-C
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

```

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 167](#).

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 167](#).

show igmp statistics

List of Syntax	Syntax on page 169 Syntax (EX Series Switch and the QFX Series) on page 169
Syntax	<pre>show igmp statistics <brief detail> <interface <i>interface-name</i>> <logical-system (all <i>logical-system-name</i>)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>show igmp statistics <brief detail> <interface <i>interface-name</i>></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>Command introduced in Junos OS Release 11.3 for the QFX Series.</p>
Description	Display Internet Group Management Protocol (IGMP) statistics.
Options	<p>none—Display IGMP statistics for all interfaces.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>interface <i>interface-name</i>—(Optional) Display IGMP statistics about the specified interface 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>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear igmp statistics on page 134
List of Sample Output	show igmp statistics on page 170 show igmp statistics interface on page 171
Output Fields	<p>Table 12 on page 169 describes the output fields for the show igmp statistics command. Output fields are listed in the approximate order in which they appear.</p>

Table 12: 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 12: 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	<pre>show igmp-snooping membership <brief detail> <interface <i>interface-name</i>> <vlan (<i>vlan-id</i> <i>vlan-name</i>)></pre>
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 about 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 about 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 175 • show igmp-snooping statistics on page 177 • show igmp-snooping vlans • Verifying IGMP Snooping (CLI Procedure) on page 38 • Configuring IGMP Snooping (CLI Procedure)
List of Sample Output	<p>show igmp-snooping membership on page 173</p> <p>show igmp-snooping membership detail on page 173</p> <p>show igmp-snooping membership vlan detail on page 174</p>
Output Fields	Table 13 on page 172 lists the output fields for the show igmp-snooping membership command. Output fields are listed in the approximate order in which they appear.

Table 13: 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 13: 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 or since the interface last flapped. For dynamic interfaces, amount of time since the first query was received on the interface or since the interface last flapped. timeout—Seconds remaining before a dynamic multicast-router interface times out. 	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. Last reporter—Last host to report membership for the multicast group. Receiver count—Number of hosts on the interface that are members of the multicast group. This field appears only if immediate-leave is configured on the VLAN. Uptime—Length of time (in hours, minutes, and seconds) a multicast group has been active on the interface. timeout—Time (in seconds) left until the entry for the multicast group is removed from the multicast group if no membership reports are received on the interface. This counter is reset to its maximum value when a membership report is received. Flags—The lowest IGMP version in use by a host that is a member of the group on the interface. If the flag static is included, the interface has been configured as static member of the multicast group. Include source—Multicast source addresses of all IGMPv3 membership reports received for the group on the interface. 	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: vlan2 Tag: 2 (Index: 3)
Router interfaces:

```

```
ge-1/0/0.0 dynamic Uptime: 00:14:24 timeout: 253
Group: 225.0.0.1
ge-1/0/17.0 259 Last reporter: 13.0.0.90 Receiver count: 1
Uptime: 00:00:19 timeout: 259 Flags: <V3-hosts>
Include source: 10.2.11.5, 10.2.11.12
```

show igmp-snooping membership vlan detail

```
user@switch> show igmp-snooping membership vlan vlan700 detail
VLAN: vlan700 Tag: 700 (Index: 52)
Router interfaces:
  ae2.0 dynamic Uptime: 16:53:13 timeout: 245
Group: 230.150.10.1
  ge-0/0/1.0 Last reporter: 100.2.188.201
  Uptime: 17:00:52 timeout: 237 Flags: <V2-hosts>
  ge-0/0/0.0 Last reporter: 100.2.188.202
  Uptime: 17:00:50 timeout: 243 Flags: <V2-hosts>
```

show igmp-snooping route

Syntax	<code>show igmp-snooping route</code> <code><brief detail></code> <code><ethernet-switching inet></code> <code><vlan (vlan-id vlan-name)></code>
Release Information	Command introduced in Junos OS Release 9.1 for EX Series switches.
Description	Display IGMP snooping route information.
Options	<p>none—Display route 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>ethernet-switching—(Optional) Display information on Layer 2 multicast routes. This is the default.</p> <p>inet—(Optional) Display information for Layer 3 multicast routes.</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 membership on page 172 • show igmp-snooping statistics on page 177 • show igmp-snooping vlans • Verifying IGMP Snooping (CLI Procedure) on page 38 • Configuring IGMP Snooping (CLI Procedure)
List of Sample Output	show igmp-snooping route vlan v18 on page 176 show igmp-snooping route detail on page 176 show igmp-snooping route inet detail on page 176
Output Fields	Table 14 on page 175 lists the output fields for the show igmp-snooping route command. Output fields are listed in the approximate order in which they appear.

Table 14: show igmp-snooping route Output Fields

Field Name	Field Description
Table	Routing table ID for virtual routing instances.
Routing Table	Routing table ID for virtual routing instances.
VLAN	Name of the VLAN on which IGMP snooping is enabled.
Group	Multicast IPv4 group address.

Table 14: 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 vlan v18

```

user@switch> show igmp-snooping route vlan v18
VLAN      Group      Next-hop
v1an18    224.0.0.0, *
v1an18    225.20.20.1, *    1539

```

show igmp-snooping route detail

```

user@switch> show igmp-snooping route detail
VLAN      Group      Next-hop
default   224.0.0.0, *
v1an100    224.0.0.0, *      1332
          Interfaces: ge-1/0/1.0
VLAN      Group      Next-hop
v1an100    226.0.0.1, *      1334
          Interfaces: ge-1/0/1.0, ge-5/0/30.0

```

show igmp-snooping route inet detail

```

user@switch> show igmp-snooping route inet detail
Routing table: 0
Group: 229.0.0.1, 171.2.60.100
  Routing next-hop: 3448
  vlan.100
  Interface: vlan.100, VLAN: vlan100, Layer 2 next-hop: 3343

```


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"> • clear igmp-snooping statistics on page 137 • show igmp-snooping membership on page 172 • show igmp-snooping route on page 175 • show igmp-snooping vlans • Verifying IGMP Snooping (CLI Procedure) on page 38 • Configuring IGMP Snooping (CLI Procedure)
List of Sample Output	show igmp-snooping statistics on page 178
Output Fields	Table 15 on page 177 lists the output fields for the show igmp-snooping statistics command. Output fields are listed in the approximate order in which they appear.

Table 15: 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.
Not local	Not used—always 0.
Receive unknown	Unknown IGMP type.
Timed out	Not used—always 0.
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 packets received that did not conform to the IGMP version 1 (IGMPv1), IGMPv2, or IGMPv3 standards.

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: 0
```

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

show multicast flow-map

List of Syntax	Syntax on page 179 Syntax (EX Series Switch and the QFX Series) on page 179
Syntax	show multicast flow-map <brief detail> <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch and the QFX Series)	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. Command introduced in Junos OS Release 11.3 for the QFX Series.
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 180 show multicast flow-map detail on page 180
Output Fields	Table 16 on page 179 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 with 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

Table 16: show multicast flow-map Output Fields (*continued*)

Field Name	Field Description	Levels of Output
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

List of Syntax	Syntax on page 181 Syntax (EX Series Switch and the QFX Series) on page 181
Syntax	show multicast interface <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switch and the QFX Series)	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. Command introduced in Junos OS Release 11.3 for the QFX Series.
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 182
Output Fields	Table 17 on page 181 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)	Amount of bandwidth, in bits per second, used by any flows that are mapped to the interface. NOTE: Adding the mapped bandwidth deduction value to the local bandwidth deduction value results in the total deduction value for the interface. This field does not appear in the output when the no QoS adjustment feature is disabled.

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

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

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        100000000               100000000
fe-0/0/3.230        20000000                18000000
fe-0/0/2.200        100000000               100000000

```

show multicast minfo

Syntax	<code>show multicast minfo</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. Command introduced in Junos OS Release 11.3 for the QFX Series.
Description	Display configuration information about IP multicast networks, including neighboring multicast router addresses.
Options	none —Display configuration information about all multicast networks. host —(Optional) Display configuration information about a particular host. Replace <i>host</i> with a hostname or IP address.
Required Privilege Level	view
List of Sample Output	show multicast minfo on page 184
Output Fields	Table 18 on page 183 describes the output fields for the show multicast minfo command. Output fields are listed in the approximate order in which they appear.

Table 18: show multicast minfo 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 minfo 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

List of Syntax	Syntax on page 185 Syntax (EX Series Switch and the QFX Series) on page 185
Syntax	<pre>show multicast next-hops <brief detail> <identifier-number> <inet inet6> <logical-system (all logical-system-name)></pre>
Syntax (EX Series Switch and the QFX Series)	<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> <p>Command introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Support for bidirectional PIM added in Junos OS Release 12.1.</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 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	show multicast next-hops on page 186 show multicast next-hops (Bidirectional PIM on page 186 show multicast next-hops brief on page 187 show multicast next-hops detail on page 187

Output Fields Table 19 on page 186 describes the output fields for the **show multicast next-hops** command. Output fields are listed in the approximate order in which they appear.

Table 19: show multicast next-hops Output Fields

Field Name	Field Description
Family	Protocol family (such as INET).
ID	Next-hop identifier of the prefix. The identifier is returned by the routing device's Packet Forwarding Engine.
Refcount	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.
Incoming interface list	List of interfaces that accept incoming traffic. Only shown for routes that do not use strict RPF-based forwarding, for example for bidirectional PIM.

Sample Output

show multicast next-hops

```
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
```

show multicast next-hops (Bidirectional PIM)

```
user@host> show multicast next-hops
Family: INET
ID      Refcount  KRefcount  Downstream interface
2097151      8          4  ge-0/0/1.0

Family: INET6
ID      Refcount  KRefcount  Downstream interface
2097157      2          1  ge-0/0/1.0

Family: Incoming interface list
ID      Refcount  KRefcount  Downstream interface
513      5          2  lo0.0
                    ge-0/0/1.0
514      5          2  lo0.0
                    ge-0/0/1.0
                    xe-4/1/0.0
515      3          1  lo0.0
                    ge-0/0/1.0
                    xe-4/1/0.0
544      1          0  lo0.0
                    xe-4/1/0.0
```

show multicast next-hops brief

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 186](#).

show multicast next-hops detail

```
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

List of Syntax	Syntax on page 188 Syntax (EX Series Switch and the QFX Series) on page 188
Syntax	<pre>show multicast pim-to-igmp-proxy <instance <i>instance-name</i>> <logical-system (all <i>logical-system-name</i>)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>show multicast pim-to-igmp-proxy <instance <i>instance-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 9.6.</p> <p>Command introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>instance option introduced in Junos OS Release 10.0.</p> <p>instance option introduced in Junos OS Release 10.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.3 for the QFX Series.</p>
Description	Display configuration information about PIM-to-IGMP message translation, also known as PIM-to-IGMP proxy.
Options	<p>none—Display configuration information about PIM-to-IGMP message translation for all routing instances.</p> <p>instance <i>instance-name</i>—(Optional) Display configuration information about PIM-to-IGMP message translation 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 pim-to-igmp-proxy on page 189 show multicast pim-to-igmp-proxy instance on page 189
Output Fields	Table 20 on page 188 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
Instance	Routing instance. Default instance is master (inet.0 routing table).
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 pim-to-igmp-proxy instance

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

show multicast pim-to-mld-proxy

List of Syntax	Syntax on page 190 Syntax (EX Series Switch and the QFX Series) on page 190
Syntax	<pre>show multicast pim-to-mld-proxy <instance <i>instance-name</i>> <logical-system (all <i>logical-system-name</i>)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>show multicast pim-to-mld-proxy <instance <i>instance-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 9.6.</p> <p>Command introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>instance option introduced in Junos OS Release 10.3.</p> <p>instance option introduced in Junos OS Release 10.3 for EX Series switches.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> <p>Command introduced in Junos OS Release 11.3 for the QFX Series.</p>
Description	Display configuration information about PIM-to-MLD message translation, also known as PIM-to-MLD proxy.
Options	<p>none—Display configuration information about PIM-to-MLD message translation for all routing instances.</p> <p>instance <i>instance-name</i>—(Optional) Display configuration information about PIM-to-MLD message translation 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 pim-to-mld-proxy on page 191 show multicast pim-to-mld-proxy instance on page 191
Output Fields	Table 21 on page 190 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 pim-to-mld-proxy instance

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

show multicast route

List of Syntax	Syntax on page 192 Syntax (EX Series Switch and the QFX Series) on page 192
Syntax	<pre>show multicast route <brief detail extensive summary> <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 and the QFX Series)	<pre>show multicast route <brief detail extensive summary> <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> <p>Command introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Support for bidirectional PIM added in Junos OS Release 12.1.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</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 summary—(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>

regular-expression—(Optional) Display information about the multicast forwarding table entries that match a UNIX OS-style regular expression.

source-prefix source-prefix—(Optional) Display the cache entries for a particular source prefix.

Required Privilege Level view

Related Documentation • [Example: Configuring Bidirectional PIM](#)

List of Sample Output [show multicast route on page 194](#)
[show multicast route \(Bidirectional PIM\) on page 195](#)
[show multicast route brief on page 195](#)
[show multicast route detail on page 196](#)
[show multicast route extensive \(Bidirectional PIM\) on page 196](#)
[show multicast route instance <instance-name> extensive on page 197](#)
[show multicast route summary on page 197](#)

Output Fields [Table 22 on page 193](#) 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
family	IPv4 address family (INET) or IPv6 address family (INET6).	All levels
Group	Group address. For any-source multicast routes, for example for bidirectional PIM, the group address includes the prefix length.	All levels
Source	Prefix and length of the source as it is in the multicast forwarding table.	All levels
Incoming interface list	List of interfaces that accept incoming traffic. Only shown for routes that do not use strict RPF-based forwarding, for example for bidirectional PIM.	All levels
Upstream interface	Name of the interface on which the packet with this source prefix is expected to arrive.	All levels
Upstream rpf interface list	When multicast-only fast reroute (MoFRR) is enabled, a PIM router propagates join messages on two upstream RPF interfaces to receive multicast traffic on both links for the same join request.	All levels
Downstream interface list	List of interface names to which the packet with this source prefix is forwarded.	All levels
Number of outgoing interfaces	Total number of outgoing interfaces for each (S,G) entry.	extensive
Session description	Name of the multicast session.	detail extensive

Table 22: show multicast route Output Fields (*continued*)

Field Name	Field Description	Level of Output
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 . NOTE: On QFX Series switches and OCX Series switches, this field does not report valid statistics.	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
Incoming interface list ID	For bidirectional PIM, incoming interface list identifier. Identifiers for interfaces that accept incoming traffic. Only shown for routes that do not use strict RPF-based forwarding, for example for bidirectional PIM.	detail extensive
Upstream protocol	The protocol that maintains the active multicast forwarding route for this group or source. When the show multicast route extensive command is used with the display-origin-protocol option, the field name is only Protocol and not Upstream Protocol . However, this field also displays the protocol that installed the active route.	detail extensive
Route type	Type of multicast route. Values can be (S,G) or (*G).	summary
Route state	Whether the group is Active or Inactive .	summary extensive
Route count	Number of multicast routes.	summary
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. A value of forever indicates routes that do not have keepalive times.	extensive
Wrong incoming interface notifications	Number of times that the upstream interface was not available.	extensive
Uptime	Time since the creation of a multicast route.	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-1/1/0.1081344

Family: INET6

```

show multicast route (Bidirectional PIM)

```

user@host> show multicast route
Family: INET

Group: 224.1.1.0/24
Source: *
Incoming interface list:
    lo0.0 ge-0/0/1.0
Downstream interface list:
    ge-0/0/1.0

Group: 224.1.3.0/24
Source: *
Incoming interface list:
    lo0.0 ge-0/0/1.0 xe-4/1/0.0
Downstream interface list:
    ge-0/0/1.0

Group: 225.1.1.0/24
Source: *
Incoming interface list:
    lo0.0 ge-0/0/1.0
Downstream interface list:
    ge-0/0/1.0

Group: 225.1.3.0/24
Source: *
Incoming interface list:
    lo0.0 ge-0/0/1.0 xe-4/1/0.0
Downstream interface list:
    ge-0/0/1.0

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 194](#) or [show multicast route \(Bidirectional PIM\) on page 195](#).

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-1/1/0.1081344
  Session description: Administratively Scoped
  Statistics: 46 kbps, 1000 pps, 921077 packets

  Next-hop ID: 262143
  Upstream protocol: PIM

Family: INET6
```

show multicast route extensive (Bidirectional PIM)

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

Group: 224.1.1.0/24
  Source: *
  Incoming interface list:
    lo0.0 ge-0/0/1.0
  Downstream interface list:
    ge-0/0/1.0
  Number of outgoing interfaces: 1
  Session description: NOB Cross media facilities
  Statistics: 0 kbps, 0 pps, 0 packets
  Next-hop ID: 2097153
  Incoming interface list ID: 585
  Upstream protocol: PIM
  Route state: Active
  Forwarding state: Forwarding
  Cache lifetime/timeout: forever
  Wrong incoming interface notifications: 0

Group: 224.1.3.0/24
```

```

Source: *
Incoming interface list:
  lo0.0 ge-0/0/1.0 xe-4/1/0.0
Downstream interface list:
  ge-0/0/1.0
Number of outgoing interfaces: 1
Session description: NOB Cross media facilities
Statistics: 0 kbps, 0 pps, 0 packets
Next-hop ID: 2097153
Incoming interface list ID: 589
Upstream protocol: PIM
Route state: Active
Forwarding state: Forwarding
Cache lifetime/timeout: forever
Wrong incoming interface notifications: 0

```

Family: INET6

show multicast route 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
Uptime: 00:00:04

```

show multicast route summary

```

user@host> show multicast route summary
Instance: master Family: INET

Route type   Route state   Route count
(S,G)        Active        2
(S,G)        Inactive       3

Instance: master Family: INET6

```

show multicast rpf

List of Syntax	Syntax on page 198 Syntax (EX Series Switch and the QFX Series) on page 198
Syntax	<pre>show multicast rpf <inet inet6> <instance <i>instance-name</i>> <logical-system (all <i>logical-system-name</i>)> <prefix> <summary></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>show multicast rpf <inet inet6> <instance <i>instance-name</i>> <prefix> <summary></pre>
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. Command introduced in Junos OS Release 11.3 for the QFX Series.
Description	Display information about multicast reverse-path-forwarding (RPF) calculations.
Options	<p>none—Display RPF calculation information for all supported address families.</p> <p>inet inet6—(Optional) Display the RPF calculation information for IPv4 or IPv6 family addresses, respectively.</p> <p>instance <i>instance-name</i>—(Optional) Display information about multicast RPF calculations 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> <p>prefix—(Optional) Display the RPF calculation information for the specified prefix.</p> <p>summary—(Optional) Display a summary of all multicast RPF information.</p>
Required Privilege Level	view
List of Sample Output	show multicast rpf on page 199 show multicast rpf inet6 on page 200 show multicast rpf prefix on page 201 show multicast rpf summary on page 201

Output Fields Table 23 on page 199 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. NOTE: The displayed interface information does not apply to bidirectional PIM RP addresses. This is because the show multicast rpf command does not take into account equal-cost paths or the designated forwarder. For accurate upstream RPF interface information, always use the show pim join extensive command when bidirectional PIM is configured.
Neighbor	Upstream RPF neighbor. NOTE: The displayed neighbor information does not apply to bidirectional PIM. This is because the show multicast rpf command does not take into account equal-cost paths or the designated forwarder. For accurate upstream RPF neighbor information, always use the show pim join extensive command when bidirectional PIM is configured.

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
```

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

List of Syntax	Syntax on page 202 Syntax (EX Series Switch and the QFX Series) on page 202
Syntax	<pre>show multicast scope <inet inet6> <instance <i>instance-name</i>> <logical-system (all <i>logical-system-name</i>)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>show multicast scope <inet inet6> <instance <i>instance-name</i>></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> <p>Command introduced in Junos OS Release 11.3 for the QFX Series.</p>
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 203 show multicast scope inet on page 203 show multicast scope inet6 on page 203
Output Fields	<p>Table 24 on page 202 describes the output fields for the show multicast scope command. Output fields are listed in the approximate order in which they appear.</p>

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.

Table 24: show multicast scope Output Fields (*continued*)

Field Name	Field Description
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 inet

```
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 inet6

```
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

List of Syntax	Syntax on page 204 Syntax (EX Series Switch and the QFX Series) on page 204
Syntax	<code>show multicast sessions</code> <code><brief detail extensive></code> <code><logical-system (all <i>logical-system-name</i>)></code> <code><<i>regular-expression</i>></code>
Syntax (EX Series Switch and the QFX Series)	<code>show multicast sessions</code> <code><brief detail extensive></code> <code><<i>regular-expression</i>></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.3 for the QFX Series.
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 205 show multicast sessions regular-expression detail on page 205
Output Fields	Table 25 on page 204 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 regular-expression detail

```

user@host> show multicast sessions "NASA TV" detail
SDP Version: 0  Originated by: -@128.223.83.33
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: fmtp: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

List of Syntax	Syntax on page 207 Syntax (EX Series Switch and the QFX Series) on page 207
Syntax	<pre>show multicast usage <brief detail> <inet inet6> <instance <i>instance-name</i>> <logical-system (all <i>logical-system-name</i>)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>show multicast usage <brief detail> <inet inet6> <instance <i>instance-name</i>></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> <p>Command introduced in Junos OS Release 11.3 for the QFX Series.</p>
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 208 show multicast usage brief on page 208 show multicast usage instance on page 208 show multicast usage detail on page 209
Output Fields	<p>Table 26 on page 208 describes the output fields for the show multicast usage command. Output fields are listed in the approximate order in which they appear.</p>

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.)
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

show multicast usage

```

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 208](#).

show multicast usage instance

```

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
...
```

show multicast usage detail

```
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

List of Syntax	Syntax on page 210 Syntax (EX Series Switch and the QFX Series) on page 210
Syntax	<pre>show pim bootstrap <instance <i>instance-name</i>> <logical-system (all <i>logical-system-name</i>)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>show pim bootstrap <instance <i>instance-name</i>></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>instance option introduced in Junos OS Release 10.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.3 for the QFX Series.</p>
Description	For sparse mode only, display information about Protocol Independent Multicast (PIM) bootstrap routers.
Options	<p>none—Display PIM bootstrap router information for all routing instances.</p> <p>instance <i>instance-name</i>—(Optional) Display information about bootstrap routers 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 bootstrap on page 211 show pim bootstrap instance on page 211
Output Fields	<p>Table 27 on page 210 describes the output fields for the show pim bootstrap command. Output fields are listed in the approximate order in which they appear.</p>

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 as elected to be the bootstrap router.
Local address	Local routing device address.
Pri	Local routing device address priority to be elected as the bootstrap router.

Table 27: show pim bootstrap Output Fields (*continued*)

Field Name	Field Description
State	Local routing device 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 instance

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

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

show pim interfaces

List of Syntax [Syntax on page 212](#)
[Syntax \(EX Series Switch and the QFX Series\) on page 212](#)

Syntax show pim interfaces
 <inet | inet6>
 <instance *instance-name*>
 <logical-system (all | *logical-system-name*)>

Syntax (EX Series Switch and the QFX Series) show pim interfaces
 <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.
 Command introduced in Junos OS Release 11.3 for the QFX Series.
 Support for bidirectional PIM added in Junos OS Release 12.1.

Description Display information about the interfaces on which Protocol Independent Multicast (PIM) is configured.

Options **none**—Display interface information for all family addresses for all routing instances.

inet | inet6—(Optional) Display interface information for IPv4 or IPv6 family addresses, respectively.

instance *instance-name*—(Optional) Display information about interfaces for a specific PIM-enabled routing instance.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level view

List of Sample Output [show pim interfaces on page 213](#)

Output Fields [Table 28 on page 212](#) 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"> • B—In bidirectional mode, multicast groups are carried across the network over bidirectional shared trees. This type of tree minimizes PIM routing state, which is especially important in networks with numerous and dispersed senders and receivers. • S—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). (Not supported on QFX Series.) • 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. (Not supported on QFX Series.) <p>When sparse-dense mode is configured, the output includes both S and D. When bidirectional-sparse mode is configured, the output includes S and B. When bidirectional-sparse-dense mode is configured, the output includes B, S, and D.</p>
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"> • Active—Bidirectional mode is enabled on the interface and on all PIM neighbors. • DR—Designated router. • NotCap—Bidirectional mode is not enabled on the interface. This can happen when bidirectional PIM is not configured locally, when one of the neighbors is not configured for bidirectional PIM, or when one of the neighbors has not implemented the bidirectional PIM protocol. • 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
Stat = Status, V = Version, NbrCnt = Neighbor Count,
S = Sparse, D = Dense, B = Bidirectional,
DR = Designated Router, P2P = Point-to-point link,

```

Active = Bidirectional is active, NotCap = Not Bidirectional Capable

Name	Stat	Mode	IP	V	State	NbrCnt	JoinCnt(sg/*g)	DR address
ge-0/3/0.0	Up	S	4	2	NotDR,NotCap	1	0/0	40.0.0.3
ge-0/3/3.50	Up	S	4	2	DR,NotCap	1	9901/100	50.0.0.2
ge-0/3/3.51	Up	S	4	2	DR,NotCap	1	0/0	51.0.0.2
pe-1/2/0.32769	Up	S	4	2	P2P,NotCap	0	0/0	

show pim join

List of Syntax [Syntax on page 215](#)
[Syntax \(EX Series Switch and the QFX Series\) on page 215](#)

Syntax `show pim join`
 `<brief | detail | extensive | summary>`
 `<bidirectional | dense | sparse>`
 `<exact>`
 `<inet | inet6>`
 `<instance instance-name>`
 `<logical-system (all | logical-system-name)>`
 `<range>`
 `<rp ip-address/prefix | source ip-address/prefix>`
 `<sg | star-g>`

Syntax (EX Series Switch and the QFX Series) `show pim join`
 `<brief | detail | extensive | summary>`
 `<dense | sparse>`
 `<exact>`
 `<inet | inet6>`
 `<instance instance-name>`
 `<range>`
 `<rp ip-address/prefix | source ip-address/prefix>`
 `<sg | star-g>`

Release Information Command introduced before Junos OS Release 7.4.
 Command introduced in Junos OS Release 9.0 for EX Series switches.
 summary option introduced in Junos OS Release 9.6.
 inet6 and **instance** options introduced in Junos OS Release 10.0 for EX Series switches.
 Support for bidirectional PIM added in Junos OS Release 12.1.
 Command introduced in Junos OS Release 11.3 for the QFX Series.
 Multiple new filter options introduced in Junos OS Release 13.2.
 Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Display information about Protocol Independent Multicast (PIM) groups for all PIM modes.

For bidirectional PIM, display information about PIM group ranges (*G-range) for each active bidirectional RP group range, in addition to each of the joined (*G) routes.

Options **none**—Display the standard information about PIM groups for all supported family addresses for all routing instances.

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

bidirectional | dense | sparse—(Optional) Display information about PIM bidirectional mode, dense mode, or sparse and source-specific multicast (SSM) mode entries.

exact—(Optional) Display information about only the group that exactly matches the specified group address.

inet | inet6—(Optional) Display PIM group information for IPv4 or IPv6 family addresses, respectively.

instance *instance-name*—(Optional) Display information about groups for the specified PIM-enabled routing instance only.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

range—(Optional) Address range of the group, specified as *prefix/prefix-length*.

rp *ip-address/prefix* | source *ip-address/prefix*—(Optional) Display information about the PIM entries with a specified rendezvous point (RP) address and prefix or with a specified source address and prefix. You can omit the prefix.

sg | star-g—(Optional) Display information about PIM (S,G) or (*,G) entries.

Required Privilege Level

view

Related Documentation

- [clear pim join on page 143](#)
- *Example: Configuring Bidirectional PIM*

List of Sample Output

[show pim join summary on page 220](#)
[show pim join \(PIM Sparse Mode\) on page 220](#)
[show pim join \(Bidirectional PIM\) on page 221](#)
[show pim join inet6 on page 221](#)
[show pim join inet6 star-g on page 222](#)
[show pim join instance <instance-name> on page 222](#)
[show pim join detail on page 222](#)
[show pim join extensive \(PIM Sparse Mode\) on page 223](#)
[show pim join extensive \(Bidirectional PIM\) on page 224](#)
[show pim join extensive \(Bidirectional PIM with a Directly Connected Phantom RP\) on page 225](#)
[show pim join instance <instance-name> extensive on page 225](#)
[show pim join extensive \(Ingress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs\) on page 226](#)
[show pim join extensive \(Egress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs\) on page 227](#)
[show pim join summary on page 228](#)
[show pim join \(PIM Sparse Mode\) on page 229](#)
[show pim join \(Bidirectional PIM\) on page 229](#)
[show pim join inet6 on page 230](#)
[show pim join inet6 star-g on page 230](#)
[show pim join instance <instance-name> on page 230](#)
[show pim join detail on page 231](#)
[show pim join extensive \(PIM Sparse Mode\) on page 231](#)
[show pim join extensive \(Bidirectional PIM\) on page 232](#)

[show pim join extensive \(Bidirectional PIM with a Directly Connected Phantom RP\) on page 233](#)

[show pim join instance <instance-name> extensive on page 233](#)

[show pim join extensive \(Ingress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs\) on page 234](#)

[show pim join extensive \(Multipoint LDP with Multicast-Only Fast Reroute\) on page 235](#)

Output Fields Table 29 on page 217 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
Bidirectional group prefix length	For bidirectional PIM, length of the IP prefix for RP group ranges.	All levels
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"> • bidirectional—Bidirectional mode entry. • 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

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

Field Name	Field Description	Level of Output
Upstream interface	<p>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).</p> <p>For bidirectional PIM, RP Link means that the interface is directly connected to a subnet that contains a phantom RP address.</p> <p>A pseudo multipoint LDP (M-LDP) interface appears on egress nodes in M-LDP point-to-multipoint LSPs with inband signaling.</p>	brief detail extensive none
Upstream neighbor	<p>Information about the upstream neighbor: Direct, Local, Unknown, or a specific IP address.</p> <p>For bidirectional PIM, Direct means that the interface is directly connected to a subnet that contains a phantom RP address.</p> <p>The multipoint LDP (M-LDP) root appears on egress nodes in M-LDP point-to-multipoint LSPs with inband signaling.</p>	extensive
Upstream state	<p>When multicast-only fast reroute (MoFRR) is configured in a PIM domain, the upstream interface for the active path. A PIM router propagates join messages on two upstream RPF interfaces to receive multicast traffic on both links for the same join request. Preference is given to two paths that do not converge to the same immediate upstream router. PIM installs appropriate multicast routes with upstream neighbors as RPF next hops with two (primary and backup) interfaces.</p>	extensive
Active upstream neighbor	<p>On the MoFRR primary path, the IP address of the neighbor that is directly connected to the active upstream interface.</p>	extensive
MoFRR Backup upstream interface	<p>The MoFRR upstream interface that is used when the primary path fails.</p> <p>When the primary path fails, the backup path is upgraded to primary, and traffic is forwarded accordingly. If there are alternate paths available, a new backup path is calculated and the appropriate multicast route is updated or installed.</p>	extensive

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

Field Name	Field Description	Level of Output
Upstream state	<p>Information about the upstream interface:</p> <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 join messages nor prune messages toward the RP, because this routing device is the rendezvous point. • Local Source—Sending neither join messages nor prune messages toward the source, because the source is locally attached to this routing device. • No Prune to RP—Automatically sent to RP when SPT and RPT are on the same path. • Prune to RP—Sending a prune to the rendezvous point. • Prune to Source—Sending a prune to the source. <p>NOTE: RP group range entries have None in the Upstream state field because RP group ranges do not trigger actual PIM join messages between routing devices.</p>	extensive
Downstream neighbors	<p>Information about downstream interfaces:</p> <ul style="list-style-type: none"> • Interface—Interface name for the downstream neighbor. A pseudo PIM-SM interface appears for all IGMP-only interfaces. A pseudo multipoint LDP (M-LDP) interface appears on ingress root nodes in M-LDP point-to-multipoint LSPs with inband signaling. • 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. • Uptime—Time since the downstream interface joined the group. • Time since last Join—Time since the last join message was received from the downstream interface. • Time since last Prune—Time since the last prune message was received from the downstream interface. 	extensive
Assert Timeout		
Assert Timeout	Length of time between assert cycles on the downstream interface. Not displayed if the assert timer is null.	extensive

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

Field Name	Field Description	Level of Output
Keepalive 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, Keepalive timeout is Infinity .	extensive
Uptime	Time since the creation of (S,G) or (*,G) state. The uptime is not refreshed every time a PIM join message is received for an existing (S,G) or (*,G) state.	extensive
Bidirectional accepting interfaces	<p>Interfaces on the router that forward bidirectional PIM traffic.</p> <p>The reasons for forwarding bidirectional PIM traffic are that the interface is the winner of the designated forwarder election (DF Winner), or the interface is the reverse path forwarding (RPF) interface toward the RP (RPF).</p>	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 (PIM Sparse Mode)

```

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 (Bidirectional PIM)

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

Group: 224.1.1.0
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.13.2
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0

Group: 224.1.3.0
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.1.3
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0 (RP Link)

Group: 225.1.1.0
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.13.2
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0

Group: 225.1.3.0
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.1.3
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0 (RP Link)

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

show pim join inet6

```
user@host> show pim join inet6
Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: ff04::e000:101
  Source: *
  RP: ::46.0.0.13
  Flags: sparse,rptree,wildcard
  Upstream interface: Local

Group: ff04::e000:101
  Source: ::1.1.1.1
  Flags: sparse
  Upstream interface: unknown (no neighbor)

Group: ff04::e800:101
  Source: ::1.1.1.1
  Flags: sparse
  Upstream interface: unknown (no neighbor)
```

```
Group: ff04::e800:101
Source: ::1.1.1.2
Flags: sparse
Upstream interface: unknown (no neighbor)
```

show pim join inet6 star-g

```
user@host> show pim join inet6 star-g
Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: ff04::e000:101
Source: *
RP: ::46.0.0.13
Flags: sparse,rptree,wildcard
Upstream interface: Local
```

show pim join instance <instance-name>

```
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 (PIM Sparse Mode)

```
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
  Uptime: 00:03:49
  Downstream neighbors:
    Interface: so-1/0/0.0
      10.111.10.2 State: Join Flags: SRW Timeout: 174
      Uptime: 00:03:49 Time since last Join: 00:01:49
    Interface: mt-1/1/0.32768
      10.10.47.100 State: Join Flags: SRW Timeout: Infinity
      Uptime: 00:03:49 Time since last Join: 00:01:49
  Number of downstream interfaces: 2

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
  Uptime: 00:03:49
  Downstream neighbors:
    Interface: so-1/0/0.0
      10.111.10.2 State: Join Flags: S Timeout: 174
      Uptime: 00:03:49 Time since last Prune: 00:01:49
    Interface: mt-1/1/0.32768
      10.10.47.100 State: Join Flags: S Timeout: Infinity
      Uptime: 00:03:49 Time since last Prune: 00:01:49
  Number of downstream interfaces: 2

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
  Uptime: 00:03:49
  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
      Uptime: 00:03:49 Time since last Prune: 00:01:49
    Interface: mt-1/1/0.32768
```

```
10.10.47.100 State: Join Flags: S   Timeout: Infinity
Uptime: 00:03:49 Time since last Prune: 00:01:49
Number of downstream interfaces: 3
```

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

show pim join extensive (Bidirectional PIM)

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

```
Group: 224.1.1.0
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.13.2
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0
  Upstream neighbor: 10.10.1.2
  Upstream state: None
  Uptime: 00:03:49
  Bidirectional accepting interfaces:
    Interface: ge-0/0/1.0    (RPF)
    Interface: lo0.0        (DF Winner)
  Number of downstream interfaces: 0

Group: 225.1.1.0
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.13.2
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0
  Upstream neighbor: 10.10.1.2
  Upstream state: None
  Uptime: 00:03:49
  Bidirectional accepting interfaces:
    Interface: ge-0/0/1.0    (RPF)
    Interface: lo0.0        (DF Winner)
  Downstream neighbors:
    Interface: lt-1/0/10.24
      10.0.24.4 State: Join   RW   Timeout: 185
    Interface: lt-1/0/10.23
      10.0.23.3 State: Join   RW   Timeout: 184
  Number of downstream interfaces: 2

Group: 225.1.3.0
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.1.3
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0 (RP Link)
  Upstream neighbor: Direct
  Upstream state: Local RP
  Uptime: 00:03:49
  Bidirectional accepting interfaces:
    Interface: ge-0/0/1.0    (RPF)
    Interface: lo0.0        (DF Winner)
    Interface: xe-4/1/0.0    (DF Winner)
  Number of downstream interfaces: 0
```


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

show pim join extensive (Bidirectional PIM with a Directly Connected Phantom RP)

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

Group: 224.1.3.0
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.1.3
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0 (RP Link)
  Upstream neighbor: Direct
  Upstream state: Local RP
  Uptime: 00:03:49
  Bidirectional accepting interfaces:
    Interface: ge-0/0/1.0      (RPF)
    Interface: lo0.0           (DF Winner)
    Interface: xe-4/1/0.0      (DF Winner)
  Number of downstream interfaces: 0
```

show pim join instance <instance-name> 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
  Uptime: 00:03:49
  Downstream neighbors:
    Interface: mt-1/1/0.32768
      10.10.47.101 State: Join Flags: SRW Timeout: 156
      Uptime: 00:03:49 Time since last Join: 00:01:49
  Number of downstream interfaces: 1

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
  Uptime: 00:14:52

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
  Uptime: 00:14:52
```

show pim join extensive (Ingress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

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

Group: 232.1.1.1
  Source: 192.168.219.11
  Flags: sparse,spt
  Upstream interface: fe-1/3/1.0
  Upstream neighbor: Direct
  Upstream state: Local Source
  Keepalive timeout:
  Uptime: 11:27:55
  Downstream neighbors:
    Interface: Pseudo-MLDP
    Interface: lt-1/2/0.25
      1.2.5.2 State: Join Flags: S   Timeout: Infinity
      Uptime: 11:27:55 Time since last Join: 11:27:55

Group: 232.1.1.2
  Source: 192.168.219.11
  Flags: sparse,spt
  Upstream interface: fe-1/3/1.0
  Upstream neighbor: Direct
  Upstream state: Local Source
  Keepalive timeout:
  Uptime: 11:27:41
  Downstream neighbors:
    Interface: Pseudo-MLDP

Group: 232.1.1.3
  Source: 192.168.219.11
  Flags: sparse,spt
  Upstream interface: fe-1/3/1.0
  Upstream neighbor: Direct
  Upstream state: Local Source
  Keepalive timeout:
  Uptime: 11:27:41
  Downstream neighbors:
    Interface: Pseudo-MLDP

Group: 232.2.2.2
  Source: 1.2.7.7
  Flags: sparse,spt
  Upstream interface: lt-1/2/0.27
  Upstream neighbor: Direct
  Upstream state: Local Source
  Keepalive timeout:
  Uptime: 11:27:25
  Downstream neighbors:
    Interface: Pseudo-MLDP

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

Group: ff3e::1:2
  Source: abcd::1:2:7:7
  Flags: sparse,spt
  Upstream interface: lt-1/2/0.27
  Upstream neighbor: Direct
```

```

Upstream state: Local Source
Keepalive timeout:
Uptime: 11:27:26
Downstream neighbors:
    Interface: Pseudo-MLDP

```

show pim join extensive (Egress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

```

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

Group: 227.1.1.1
  Source: *
  RP: 1.1.1.1
  Flags: sparse,rptree,wildcard
  Upstream interface: Local
  Upstream neighbor: Local
  Upstream state: Local RP
  Uptime: 11:31:33
  Downstream neighbors:
    Interface: fe-1/3/0.0
      192.168.209.9 State: Join Flags: SRW Timeout: Infinity
      Uptime: 11:31:33 Time since last Join: 11:31:32

Group: 232.1.1.1
  Source: 192.168.219.11
  Flags: sparse,spt
  Upstream protocol: MLDP
  Upstream interface: Pseudo MLDP
  Upstream neighbor: MLDP LSP root <1.1.1.2>
  Upstream state: Join to Source
  Keepalive timeout:
  Uptime: 11:31:32
  Downstream neighbors:
    Interface: so-0/1/3.0
      192.168.92.9 State: Join Flags: S Timeout: Infinity
      Uptime: 11:31:30 Time since last Join: 11:31:30
    Downstream neighbors:
      Interface: fe-1/3/0.0
        192.168.209.9 State: Join Flags: S Timeout: Infinity
        Uptime: 11:31:32 Time since last Join: 11:31:32

Group: 232.1.1.2
  Source: 192.168.219.11
  Flags: sparse,spt
  Upstream protocol: MLDP
  Upstream interface: Pseudo MLDP
  Upstream neighbor: MLDP LSP root <1.1.1.2>
  Upstream state: Join to Source
  Keepalive timeout:
  Uptime: 11:31:32
  Downstream neighbors:
    Interface: so-0/1/3.0
      192.168.92.9 State: Join Flags: S Timeout: Infinity
      Uptime: 11:31:30 Time since last Join: 11:31:30
    Downstream neighbors:
      Interface: lt-1/2/0.14
        1.1.4.4 State: Join Flags: S Timeout: 177
        Uptime: 11:30:33 Time since last Join: 00:00:33
    Downstream neighbors:

```

```

Interface: fe-1/3/0.0
  192.168.209.9 State: Join Flags: S   Timeout: Infinity
  Uptime: 11:31:32 Time since last Join: 11:31:32

Group: 232.1.1.3
  Source: 192.168.219.11
  Flags: sparse,spt
  Upstream protocol: MLDP
  Upstream interface: Pseudo MLDP
  Upstream neighbor: MLDP LSP root <1.1.1.2>
  Upstream state: Join to Source
  Keepalive timeout:
  Uptime: 11:31:32
  Downstream neighbors:
    Interface: fe-1/3/0.0
      192.168.209.9 State: Join Flags: S   Timeout: Infinity
      Uptime: 11:31:32 Time since last Join: 11:31:32

Group: 232.2.2.2
  Source: 1.2.7.7
  Flags: sparse,spt
  Upstream protocol: MLDP
  Upstream interface: Pseudo MLDP
  Upstream neighbor: MLDP LSP root <1.1.1.2>
  Upstream state: Join to Source
  Keepalive timeout:
  Uptime: 11:31:30
  Downstream neighbors:
    Interface: so-0/1/3.0
      192.168.92.9 State: Join Flags: S   Timeout: Infinity
      Uptime: 11:31:30 Time since last Join: 11:31:30

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

Group: ff3e::1:2
  Source: abcd::1:2:7:7
  Flags: sparse,spt
  Upstream protocol: MLDP
  Upstream interface: Pseudo MLDP
  Upstream neighbor: MLDP LSP root <1.1.1.2>
  Upstream state: Join to Source
  Keepalive timeout:
  Uptime: 11:31:32
  Downstream neighbors:
    Interface: fe-1/3/0.0
      fe80::21f:12ff:fea5:c4db State: Join Flags: S   Timeout: Infinity
      Uptime: 11:31:32 Time since last Join: 11:31:32

```

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 (PIM Sparse Mode)

```

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 (Bidirectional PIM)

```

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

Group: 224.1.1.0
Bidirectional group prefix length: 24
Source: *
RP: 10.10.13.2
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0

Group: 224.1.3.0
Bidirectional group prefix length: 24
Source: *
RP: 10.10.1.3
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0 (RP Link)

Group: 225.1.1.0
Bidirectional group prefix length: 24
Source: *
RP: 10.10.13.2
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0

Group: 225.1.3.0
Bidirectional group prefix length: 24
Source: *
RP: 10.10.1.3
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0 (RP Link)

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

```

show pim join inet6

```
user@host> show pim join inet6
Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: ff04::e000:101
  Source: *
  RP: ::46.0.0.13
  Flags: sparse,rptree,wildcard
  Upstream interface: Local

Group: ff04::e000:101
  Source: ::1.1.1.1
  Flags: sparse
  Upstream interface: unknown (no neighbor)

Group: ff04::e800:101
  Source: ::1.1.1.1
  Flags: sparse
  Upstream interface: unknown (no neighbor)

Group: ff04::e800:101
  Source: ::1.1.1.2
  Flags: sparse
  Upstream interface: unknown (no neighbor)
```

show pim join inet6 star-g

```
user@host> show pim join inet6 star-g
Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: ff04::e000:101
  Source: *
  RP: ::46.0.0.13
  Flags: sparse,rptree,wildcard
  Upstream interface: Local
```

show pim join instance <instance-name>

```
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 (PIM Sparse Mode)

```
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
  Uptime: 00:03:49
  Downstream neighbors:
    Interface: so-1/0/0.0
      10.111.10.2 State: Join Flags: SRW Timeout: 174
      Uptime: 00:03:49 Time since last Join: 00:01:49
    Interface: mt-1/1/0.32768
      10.10.47.100 State: Join Flags: SRW Timeout: Infinity
      Uptime: 00:03:49 Time since last Join: 00:01:49
  Number of downstream interfaces: 2

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
  Uptime: 00:03:49
  Downstream neighbors:
    Interface: so-1/0/0.0
```

```

    10.111.10.2 State: Join Flags: S Timeout: 174
    Uptime: 00:03:49 Time since last Prune: 00:01:49
    Interface: mt-1/1/0.32768
    10.10.47.100 State: Join Flags: S Timeout: Infinity
    Uptime: 00:03:49 Time since last Prune: 00:01:49
    Number of downstream interfaces: 2

```

```

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
Uptime: 00:03:49
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
    Uptime: 00:03:49 Time since last Prune: 00:01:49
  Interface: mt-1/1/0.32768
    10.10.47.100 State: Join Flags: S Timeout: Infinity
    Uptime: 00:03:49 Time since last Prune: 00:01:49
  Number of downstream interfaces: 3

```

```

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

```

show pim join extensive (Bidirectional PIM)

```

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

```

```

Group: 224.1.1.0
Bidirectional group prefix length: 24
Source: *
RP: 10.10.13.2
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0
Upstream neighbor: 10.10.1.2
Upstream state: None
Uptime: 00:03:49
Bidirectional accepting interfaces:
  Interface: ge-0/0/1.0 (RPF)
  Interface: lo0.0 (DF Winner)
Number of downstream interfaces: 0

```

```

Group: 225.1.1.0
Bidirectional group prefix length: 24
Source: *
RP: 10.10.13.2
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0
Upstream neighbor: 10.10.1.2
Upstream state: None
Uptime: 00:03:49
Bidirectional accepting interfaces:
  Interface: ge-0/0/1.0 (RPF)
  Interface: lo0.0 (DF Winner)

```



```

Downstream neighbors:
  Interface: lt-1/0/10.24
    10.0.24.4 State: Join   RW   Timeout: 185
  Interface: lt-1/0/10.23
    10.0.23.3 State: Join   RW   Timeout: 184
Number of downstream interfaces: 2

Group: 225.1.3.0
Bidirectional group prefix length: 24
Source: *
RP: 10.10.1.3
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0 (RP Link)
Upstream neighbor: Direct
Upstream state: Local RP
Uptime: 00:03:49
Bidirectional accepting interfaces:
  Interface: ge-0/0/1.0      (RPF)
  Interface: lo0.0           (DF Winner)
  Interface: xe-4/1/0.0      (DF Winner)
Number of downstream interfaces: 0

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

```

show pim join extensive (Bidirectional PIM with a Directly Connected Phantom RP)

```

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

Group: 224.1.3.0
Bidirectional group prefix length: 24
Source: *
RP: 10.10.1.3
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0 (RP Link)
Upstream neighbor: Direct
Upstream state: Local RP
Uptime: 00:03:49
Bidirectional accepting interfaces:
  Interface: ge-0/0/1.0      (RPF)
  Interface: lo0.0           (DF Winner)
  Interface: xe-4/1/0.0      (DF Winner)
Number of downstream interfaces: 0

```

show pim join instance <instance-name> 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
Uptime: 00:03:49
Downstream neighbors:

```

```
Interface: mt-1/1/0.32768
10.10.47.101 State: Join Flags: SRW Timeout: 156
Uptime: 00:03:49 Time since last Join: 00:01:49
Number of downstream interfaces: 1
```

```
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
Uptime: 00:14:52
```

```
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
Uptime: 00:14:52
```

show pim join extensive (Ingress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

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

Group: 232.1.1.1
Source: 192.168.219.11
Flags: sparse,spt
Upstream interface: fe-1/3/1.0
Upstream neighbor: Direct
Upstream state: Local Source
Keepalive timeout:
Uptime: 11:27:55
Downstream neighbors:
Interface: Pseudo-MLDP
Interface: lt-1/2/0.25
1.2.5.2 State: Join Flags: S Timeout: Infinity
Uptime: 11:27:55 Time since last Join: 11:27:55

Group: 232.1.1.2
Source: 192.168.219.11
Flags: sparse,spt
Upstream interface: fe-1/3/1.0
Upstream neighbor: Direct
Upstream state: Local Source
Keepalive timeout:
Uptime: 11:27:41
Downstream neighbors:
Interface: Pseudo-MLDP

Group: 232.1.1.3
Source: 192.168.219.11
Flags: sparse,spt
Upstream interface: fe-1/3/1.0
Upstream neighbor: Direct
Upstream state: Local Source
Keepalive timeout:
```

```

Uptime: 11:27:41
Downstream neighbors:
  Interface: Pseudo-MLDP

Group: 232.2.2.2
Source: 1.2.7.7
Flags: sparse,spt
Upstream interface: lt-1/2/0.27
Upstream neighbor: Direct
Upstream state: Local Source
Keepalive timeout:
Uptime: 11:27:25
Downstream neighbors:
  Interface: Pseudo-MLDP

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

Group: ff3e::1:2
Source: abcd::1:2:7:7
Flags: sparse,spt
Upstream interface: lt-1/2/0.27
Upstream neighbor: Direct
Upstream state: Local Source
Keepalive timeout:
Uptime: 11:27:26
Downstream neighbors:
  Interface: Pseudo-MLDP

```

show pim join extensive (Multipoint LDP with Multicast-Only Fast Reroute)

```

user@host> show pim join 225.1.1.1 extensive sg
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 225.1.1.1
Source: 10.0.0.1
Flags: sparse,spt
Active upstream interface: fe-1/2/13.0
Active upstream neighbor: 10.0.0.9
MoFRR Backup upstream interface: fe-1/2/14.0
MoFRR Backup upstream neighbor: 10.0.0.21
Upstream state: Join to Source, No Prune to RP
Keepalive timeout: 354
Uptime: 00:00:06
Downstream neighbors:
  Interface: fe-1/2/15.0
    10.0.0.13 State: Join Flags: S   Timeout: Infinity
    Uptime: 00:00:06 Time since last Join: 00:00:06
Number of downstream interfaces: 1

```

show pim neighbors

List of Syntax	Syntax on page 236 Syntax (EX Series Switch and the QFX Series) on page 236
Syntax	<pre>show pim neighbors <brief detail> <inet inet6> <instance <i>instance-name</i>> <logical-system (all <i>logical-system-name</i>)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>show pim neighbors <brief detail> <inet inet6> <instance <i>instance-name</i>></pre>
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. Command introduced in Junos OS Release 11.3 for the QFX Series. Support for bidirectional PIM added in Junos OS Release 12.1. Support for the instance all option added in Junos OS Release 12.1. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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 the main instance.</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> all)—(Optional) Display information about neighbors for the specified PIM-enabled routing instance or for all routing instances.</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 238 show pim neighbors brief on page 238 show pim neighbors instance on page 238 show pim neighbors detail on page 238 show pim neighbors detail (With BFD) on page 239
Output Fields	Table 30 on page 237 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
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. • G—Generation Identifier. • H—Hello Option Holdtime. • L—Hello Option LAN Prune Delay. • P—Hello Option DR Priority. • T—Tracking bit. 	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 routing device.	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-digit or 10-digit number used to tag hello messages.	detail
Hello Option Bi-Directional PIM supported	Neighbor can process bidirectional PIM 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

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

Field Name	Field Description	Level of Output
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, T = Tracking bit

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 238](#).

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, T = Tracking bit

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: ge-0/0/1.0

Address: 10.10.1.1, IPv4, PIM v2, Mode: SparseDense, sg Join Count: 0, ts
Join Count: 2
Hello Option Holdtime: 65535 seconds
Hello Option DR Priority: 1
Hello Option Generation ID: 2053759302
Hello Option Bi-Directional PIM supported
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Join Suppression supported

```

```

Address: 10.10.1.2, IPv4, PIM v2, sg Join Count: 0, tsg Join Count: 2
  BFD: Disabled
  Hello Option Holdtime: 105 seconds 93 remaining
  Hello Option DR Priority: 1
  Hello Option Generation ID: 1734018161
  Hello Option Bi-Directional PIM supported
  Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
                                Join Suppression supported

```

```
Interface: lo0.0
```

```

Address: 10.255.179.246, IPv4, PIM v2, Mode: SparseDense, sg Join Count:
0, tsg Join Count: 0
  Hello Option Holdtime: 65535 seconds
  Hello Option DR Priority: 1
  Hello Option Generation ID: 1997462267
  Hello Option Bi-Directional PIM supported
  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

List of Syntax	Syntax on page 240 Syntax (EX Series Switch and the QFX Series) on page 240
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 and the QFX Series)	<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> <p>Command introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Support for bidirectional PIM added in Junos OS Release 12.1.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</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
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Bidirectional PIM
List of Sample Output	show pim rps on page 243 show pim rps brief on page 243

[show pim rps <group-address> on page 243](#)
[show pim rps <group-address> \(Bidirectional PIM\) on page 243](#)
[show pim rps <group-address> \(PIM Dense Mode\) on page 244](#)
[show pim rps <group-address> \(SSM Range Without asm-override-ssm Configured\) on page 244](#)
[show pim rps <group-address> \(SSM Range With asm-override-ssm Configured and a Sparse-Mode RP\) on page 244](#)
[show pim rps <group-address> \(SSM Range With asm-override-ssm Configured and a Bidirectional RP\) on page 244](#)
[show pim rps instance on page 244](#)
[show pim rps extensive \(PIM Sparse Mode\) on page 244](#)
[show pim rps extensive \(Bidirectional PIM\) on page 245](#)
[show pim rps extensive \(PIM Anycast RP in Use\) on page 245](#)

Output Fields Table 31 on page 241 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 or Address 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
Mode	The PIM mode of the RP: bidirectional or sparse. If a sparse and bidirectional RPs are configured with the same RP address, they appear as separate entries in both formats.	All levels

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

Field Name	Field Description	Level of Output
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 Junos OS finds and initializes the interface. For bidirectional RPs, the Device Index output field is omitted because bidirectional RPs do not require encapsulation and de-encapsulation interfaces.	detail extensive
Subunit	Logical unit number of the interface. For bidirectional RPs, the Subunit output field is omitted because bidirectional RPs do not require encapsulation and de-encapsulation interfaces.	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. For bidirectional RPs, the Interface output field is omitted because bidirectional RPs do not require encapsulation and de-encapsulation interfaces.	detail extensive
Group Ranges	Addresses of groups that this RP spans.	detail extensive <i>group-address</i>
Active groups using RP	Number of groups currently using this RP.	detail extensive
total	Total number of active groups for this RP.	detail extensive
Register State for RP	Current register state for each group: <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

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

Field Name	Field Description	Level of Output
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
RP selected	For sparse mode and bidirectional mode, the identity of the RP for the specified group address.	<i>group-address</i>

Sample Output

show pim rps

```

user@host> show pim rps
Instance: PIM.master
Address family INET
RP address      Type      Mode    Holdtime Timeout Groups  Group prefixes
10.10.1.3       static    bidir   150      None     2  224.1.3.0/24
                225.1.3.0/24
10.10.13.2      static    bidir   150      None     2  224.1.1.0/24
                225.1.1.0/24

```

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 243](#).

show pim rps <group-address>

```

user@host> show pim rps 235.100.100.0
Instance: PIM.master
Instance: PIM.master

RP selected: 100.100.100.100

```

show pim rps <group-address> (Bidirectional PIM)

```

user@host> show pim rps 224.1.1.1
Instance: PIM.master

224.1.0.0/16
11.4.12.75 (Bidirectional)

RP selected: 11.4.12.75

```

show pim rps <group-address> (PIM Dense Mode)

```
user@host> show pim rps 224.1.1.1
Instance: PIM.master

Dense Mode active for group 224.1.1.1
```

show pim rps <group-address> (SSM Range Without asm-override-ssm Configured)

```
user@host> show pim rps 224.1.1.1
Instance: PIM.master

Source-specific Mode (SSM) active for group 224.1.1.1
```

show pim rps <group-address> (SSM Range With asm-override-ssm Configured and a Sparse-Mode RP)

```
user@host> show pim rps 224.1.1.1
Instance: PIM.master

Source-specific Mode (SSM) active with Sparse Mode ASM override for group 224.1.1.1

224.1.0.0/16
    11.4.12.75

RP selected: 11.4.12.75
```

show pim rps <group-address> (SSM Range With asm-override-ssm Configured and a Bidirectional RP)

```
user@host> show pim rps 224.1.1.1
Instance: PIM.master

Source-specific Mode (SSM) active with Sparse Mode ASM override for group 224.1.1.1

224.1.0.0/16
    11.4.12.75 (Bidirectional)

RP selected: (null)
```

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 (PIM Sparse Mode)

```
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 (Bidirectional PIM)

```

user@host> show pim rps extensive

```

```

Instance: PIM.master

```

```

Address family INET

```

```

RP: 10.10.1.3

```

```

Learned via: static configuration

```

```

Mode: Bidirectional

```

```

Time Active: 01:58:07

```

```

Holdtime: 150

```

```

Group Ranges:

```

```

    224.1.3.0/24

```

```

    225.1.3.0/24

```

```

RP: 10.10.13.2

```

```

Learned via: static configuration

```

```

Mode: Bidirectional

```

```

Time Active: 01:58:07

```

```

Holdtime: 150

```

```

Group Ranges:

```

```

    224.1.1.0/24

```

```

    225.1.1.0/24

```

show pim rps extensive (PIM Anycast RP in Use)

```

user@host> show pim rps extensive

```

```

Instance: PIM.master

```

```

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

List of Syntax	Syntax on page 247 Syntax (EX Series Switch and the QFX Series) on page 247
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 and the QFX Series)	<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> <p>Command introduced in Junos OS Release 11.3 for the QFX Series.</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 248 show pim source brief on page 248 show pim source detail on page 248
Output Fields	<p>Table 32 on page 248 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.
Source	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.
Upstream Neighbor	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 248](#).

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

List of Syntax	Syntax on page 250 Syntax (EX Series Switch and the QFX Series) on page 250
Syntax	<pre>show pim statistics <inet inet6> <instance <i>instance-name</i>> <interface <i>interface-name</i>> <logical-system (all <i>logical-system-name</i>)></pre>
Syntax (EX Series Switch and the QFX Series)	<pre>show pim statistics <inet inet6> <instance <i>instance-name</i>> <interface <i>interface-name</i>></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> <p>Command introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Support for bidirectional PIM added in Junos OS Release 12.1.</p>
Description	Display Protocol Independent Multicast (PIM) statistics.
Options	<p>none—Display PIM statistics.</p> <p>inet inet6—(Optional) Display IPv4 or IPv6 PIM statistics, respectively.</p> <p>instance <i>instance-name</i>—(Optional) Display statistics for a specific routing instance enabled by Protocol Independent Multicast (PIM).</p> <p>interface <i>interface-name</i>—(Optional) Display statistics about the specified 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	view
Related Documentation	<ul style="list-style-type: none">• clear pim statistics on page 147
List of Sample Output	<p>show pim statistics on page 256</p> <p>show pim statistics inet interface <interface-name> on page 257</p> <p>show pim statistics inet6 interface <interface-name> on page 258</p> <p>show pim statistics interface <interface-name> on page 258</p>
Output Fields	<p>Table 33 on page 251 describes the output fields for the show pim statistics command. Output fields are listed in the approximate order in which they appear.</p>

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 acknowledgment packets.
V2 Candidate RP	PIM version 2 candidate RP packets.

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

Field Name	Field Description
V2 State Refresh	PIM version 2 control messages related to PIM dense mode (PIM-DM) state refresh. State refresh is an extension to PIM-DM. It not supported in Junos OS.
V2 DF Election	PIM version 2 send and receive messages associated with bidirectional PIM designated forwarder election.
V1 Query	PIM version 1 query packets.
V1 Register	PIM version 1 register packets.
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 acknowledgment 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.

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

Field Name	Field Description
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.
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 the 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 received 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 for invalid group	Number of join or prune messages received for invalid multicast group addresses.

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

Field Name	Field Description
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 acknowledgment messages received for which the router or switch 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.
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 OS 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 encaps 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.

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

Field Name	Field Description
RP mode mismatch	RP mode (sparse or bidirectional) mismatches encountered when processing join and prune messages.
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.
Embedded-RP limit exceed	Number of times the limit configured 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 received 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.
Rx Bidir Join/Prune on non-Bidir if	Error counter for join and prune messages received on non-bidirectional PIM interfaces.

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

Field Name	Field Description
Rx Bidir Join/Prune on non-DF if	Error counter for join and prune messages received on non-designated forwarder interfaces.

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
V2 State Refresh       0            0          0
V2 DF Election         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                    0
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 for invalid group	5
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
Rx illegal TTL	0
Rx illegal destination address	0
No RP	0
No register encap if	0
No route upstream	0
Nexthop Unusable	0
RP mismatch	0
RP mode mismatch	0
RPF neighbor unknown	0
Rx Joins/Prunes filtered	0
Tx 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
Rx Bidir Join/Prune on non-Bidir if	0
Rx Bidir Join/Prune on non-DF if	0

Sample Output

show pim statistics inet interface <interface-name>

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

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 inet6 interface <interface-name>

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

PIM Interface statistics for ge-0/3/0.0

PIM Message type	Received	Sent	Rx errors
V2 Hello	0	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 interface <interface-name>

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

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

