

Multicast on EX9200 Switches

Release
15.1



Modified: 2015-06-04

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 on EX9200 Switches

15.1

Copyright © 2015, 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	xvii
	Documentation and Release Notes	xvii
	Supported Platforms	xvii
	Using the Examples in This Manual	xvii
	Merging a Full Example	xviii
	Merging a Snippet	xviii
	Documentation Conventions	xix
	Documentation Feedback	xxi
	Requesting Technical Support	xxi
	Self-Help Online Tools and Resources	xxi
	Opening a Case with JTAC	xxii
Part 1	Overview	
Chapter 1	Understanding Multicast	3
	Multicast Overview	3
	Comparing Multicast to Unicast	3
	IP Multicast Uses	5
	IP Multicast Terminology	6
	Reverse-Path Forwarding for Loop Prevention	7
	Shortest-Path Tree for Loop Prevention	7
	Administrative Scoping for Loop Prevention	7
	Multicast Leaf and Branch Terminology	7
	IP Multicast Addressing	8
	Multicast Addresses	9
	Layer 2 Frames and IPv4 Multicast Addresses	9
	Multicast Interface Lists	11
	Multicast Routing Protocols	11
	T Series Router Multicast Performance	14
	Supported IP Multicast Protocol Standards	15
Part 2	Managing Group Membership	
Chapter 2	IGMP	19
	Configuring IGMP	19
	Understanding Group Membership Protocols	19
	Understanding IGMP	21
	Configuring IGMP	23
	Enabling IGMP	24
	Modifying the IGMP Host-Query Message Interval	25
	Modifying the IGMP Query Response Interval	26

	Specifying Immediate-Leave Host Removal for IGMP	26
	Filtering Unwanted IGMP Reports at the IGMP Interface Level	27
	Accepting IGMP Messages from Remote Subnetworks	28
	Modifying the IGMP Last-Member Query Interval	29
	Modifying the IGMP Robustness Variable	29
	Limiting the Maximum IGMP Message Rate	30
	Changing the IGMP Version	31
	Enabling IGMP Static Group Membership	31
	Recording IGMP Join and Leave Events	37
	Limiting the Number of IGMP Multicast Group Joins on Logical Interfaces	39
	Tracing IGMP Protocol Traffic	40
	Disabling IGMP	42
	IGMP and Nonstop Active Routing	42
Chapter 3	Managing Group Membership with MLD (IPv6)	43
	Understanding MLD	43
	Understanding MLD Snooping	46
	How MLD Snooping Works	47
	MLD Message Types	48
	How Hosts Join and Leave Multicast Groups	48
	Support for MLDv2 Multicast Sources	49
	MLD Snooping and Forwarding Interfaces	49
	General Forwarding Rules	50
	Examples of MLD Snooping Multicast Forwarding	50
	Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts	50
	Scenario 2: Switch Forwarding Multicast Traffic to Another Switch	51
	Scenario 3: Switch Connected to Hosts Only (No MLD Querier)	52
	Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs	53
	Configuring MLD Snooping on a VLAN (CLI Procedure)	54
	Enabling or Disabling MLD Snooping on VLANs	55
	Configuring the MLD Version	56
	Enabling Immediate Leave	56
	Configuring an Interface as a Multicast-Router Interface	57
	Configuring Static Group Membership on an Interface	58
	Changing the Timer and Counter Values	59
	Example: Configuring MLD Snooping on EX Series Switches	60
	Verifying MLD Snooping	63
	Verifying MLD Snooping Memberships	64
	Verifying MLD Snooping Interfaces	64
	Viewing MLD Snooping Statistics	65
	Viewing MLD Snooping Routing Information	66
	Configuring MLD Snooping Tracing Operations (CLI Procedure)	67
	Configuring Tracing Operations	68
	Viewing, Stopping, and Restarting Tracing Operations	68

Part 3	Configuring Protocol Independent Multicast	
Chapter 4	Understanding PIM	73
	PIM Overview	73
	Basic PIM Network Components	75
Chapter 5	Configuring PIM Basics	77
	Configuring Basic PIM Settings	77
	PIM Configuration Statements	77
	Changing the PIM Version	80
	Modifying the PIM Hello Interval	80
	Preserving Multicast Performance by Disabling Response to the ping Utility	81
	PIM on Aggregated Interfaces	82
	Configuring PIM Trace Options	82
	Disabling PIM	84
	Disabling the PIM Protocol	85
	Disabling PIM on an Interface	85
	Disabling PIM for a Family	86
	Disabling PIM for a Rendezvous Point	86
	Verifying a Multicast Configuration	87
	Verifying SAP and SDP Addresses and Ports	87
	Verifying the IGMP Version	87
	Verifying the PIM Mode and Interface Configuration	88
	Verifying the PIM RP Configuration	88
	Verifying the RPF Routing Table Configuration	88
	Configuring Multiple Instances of PIM	89
	Configuring a Designated Router for PIM	90
	Configuring Interface Priority for PIM Designated Router Selection	90
	Configuring PIM Designated Router Election on Point-to-Point Links	91
Chapter 6	Routing Content to Densely Clustered Receivers with PIM Dense Mode	93
	Configuring PIM Dense Mode	93
	Understanding PIM Dense Mode	93
	Configuring PIM Dense Mode Properties	95
	Configuring PIM Sparse-Dense Mode	96
	Understanding PIM Sparse-Dense Mode	96
	Mixing PIM Sparse and Dense Modes	96
	Configuring PIM Sparse-Dense Mode Properties	97
Chapter 7	Routing Content to Larger, Sparser Groups with PIM Sparse Mode	99
	Configuring PIM Auto-RP	99
	Understanding PIM Auto-RP	99
	Configuring PIM Auto-RP	99
	Configuring Embedded RP	103
	Understanding Embedded RP for IPv6 Multicast	104
	Configuring PIM Embedded RP for IPv6	105

	Configuring Static RP	106
	Understanding Static RP	106
	Configuring Local PIM RPs	107
	Example: Configuring PIM Sparse Mode and RP Static IP Addresses	109
	Configuring the Static PIM RP Address on the Non-RP Routing Device	111
	Configuring PIM Bootstrap Router	113
	Understanding the PIM Bootstrap Router	113
	Configuring PIM Bootstrap Properties for IPv4	113
	Configuring PIM Bootstrap Properties for IPv4 or IPv6	114
	Example: Rejecting PIM Bootstrap Messages at the Boundary of a PIM Domain	116
	Example: Configuring PIM BSR Filters	117
	Configuring PIM Filtering	117
	Understanding Multicast Message Filters	117
	Filtering MAC Addresses	118
	Filtering RP and DR Register Messages	118
	Filtering MSDP SA Messages	119
	Configuring Interface-Level PIM Neighbor Policies	120
	Filtering Outgoing PIM Join Messages	121
	Example: Stopping Outgoing PIM Register Messages on a Designated Router	122
	Filtering Incoming PIM Join Messages	124
	Example: Rejecting Incoming PIM Register Messages on RP Routers	126
	Configuring Register Message Filters on a PIM RP and DR	128
Chapter 8	Rapidly Detecting Communication Failures with PIM and BFD Protocol	131
	Configuring PIM and the Bidirectional Forwarding Detection (BFD) Protocol	131
	Understanding Bidirectional Forwarding Detection Authentication for PIM	131
	BFD Authentication Algorithms	132
	Security Authentication Keychains	132
	Strict Versus Loose Authentication	133
	Configuring BFD for PIM	133
	Configuring BFD Authentication for PIM	134
	Configuring BFD Authentication Parameters	135
	Viewing Authentication Information for BFD Sessions	136
	Example: Configuring BFD Liveness Detection for PIM IPv6	137
Part 4	Configuring Multicast Routing Protocols	
Chapter 9	Connecting Routing Domains Using MSDP	147
	Configuring Multiple Instances of MSDP	147
Part 5	Configuring Multicast VPNs	
Chapter 10	Configuring PIM Join Load Balancing	151
	PIM Join Load Balancing on Multipath MVPN Routes Overview	151

Part 6	Configuring General Multicast Options	
Chapter 11	Enabling Multicast Between Layer 2 and Layer 3 Devices Using Snooping	159
	PIM Snooping for VPLS	159
	Understanding PIM Snooping for VPLS	159
	Example: Configuring PIM Snooping for VPLS	160
Part 7	Configuration Statements and Operational Commands	
Chapter 12	Configuration Statements: IGMP	173
	igmp	175
	accounting (Protocols IGMP Interface)	176
	accounting (Protocols IGMP)	176
	disable (Protocols IGMP)	177
	exclude (Protocols IGMP)	177
	group (Protocols IGMP)	178
	group-count (Protocols IGMP)	179
	group-increment (Protocols IGMP)	179
	group-limit (IGMP)	180
	group-policy (Protocols IGMP)	181
	group-threshold (Protocols IGMP Interface)	182
	immediate-leave (Protocols IGMP)	183
	interface (Protocols IGMP)	184
	log-interval (Protocols IGMP Interface)	185
	maximum-transmit-rate (Protocols IGMP)	186
	oif-map (IGMP Interface)	186
	passive (IGMP)	187
	promiscuous-mode (Protocols IGMP)	188
	query-interval (Protocols IGMP)	189
	query-last-member-interval (Protocols IGMP)	190
	query-response-interval (Protocols IGMP)	191
	robust-count (Protocols IGMP)	192
	source (Protocols IGMP)	193
	source-count (Protocols IGMP)	194
	source-increment (Protocols IGMP)	195
	ssm-map (Protocols IGMP)	195
	ssm-map-policy (IGMP)	196
	static (Protocols IGMP)	197
	traceoptions (Protocols IGMP)	198
	version (Protocols IGMP)	200
Chapter 13	Configuration Statements: IGMP Snooping	201
	igmp-snooping	202
	group (Bridge Domains)	203
	group-limit (IGMP and MLD Snooping)	204
	host-only-interface	205
	immediate-leave (Bridge Domains)	206
	interface (Bridge Domains)	208
	multicast-router-interface (IGMP Snooping)	209

	proxy (Bridge Domains)	210
	query-interval (Bridge Domains)	211
	query-last-member-interval (Bridge Domains)	212
	query-response-interval (Bridge Domains)	213
	robust-count (Bridge Domains)	214
	source (Bridge Domains)	215
	source-address	215
	static (Bridge Domains)	216
	traceoptions (Protocols IGMP Snooping)	217
	vlan (Bridge Domains)	219
Chapter 14	Configuration Statements: MLD	221
	mld	222
	accounting (Protocols MLD Interface)	223
	accounting (Protocols MLD)	223
	disable (Protocols MLD)	224
	exclude (Protocols MLD)	224
	group (Protocols MLD)	225
	group-count (Protocols MLD)	226
	group-increment (Protocols MLD)	226
	group-limit (MLD)	227
	group-policy (Protocols MLD)	228
	group-threshold (Protocols MLD Interface)	229
	immediate-leave (Protocols MLD)	230
	interface (Protocols MLD)	231
	log-interval (Protocols MLD Interface)	232
	maximum-transmit-rate (Protocols MLD)	233
	oif-map (MLD Interface)	233
	passive (MLD)	234
	query-interval (Protocols MLD)	235
	query-last-member-interval (Protocols MLD)	236
	query-response-interval (Protocols MLD)	237
	robust-count (Protocols MLD)	238
	source (Protocols MLD)	238
	source-count (Protocols MLD)	239
	source-increment (Protocols MLD)	239
	ssm-map (Protocols MLD)	240
	ssm-map-policy (MLD)	240
	static (Protocols MLD)	241
	version (Protocols MLD)	242
Chapter 15	Configuration Statements: MLD Snooping	243
	mld-snooping	244
	group (MLD Snooping)	245
	group-limit (MLD)	246
	host-only-interface	247
	immediate-leave (MLD Snooping)	248
	interface (MLD Snooping)	249
	multicast-router-interface (MLD Snooping)	250
	qualified-vlan (MLD Snooping)	250

	query-interval (Protocols MLD)	251
	query-last-member-interval (Protocols MLD)	252
	query-response-interval (Protocols MLD)	253
	robust-count (MLD Snooping)	254
	static (MLD Snooping)	255
	traceoptions (MLD Snooping)	256
	vlan (MLD Snooping)	259
Chapter 16	Configuration Statements: MSDP	261
	msdp	262
	active-source-limit	264
	authentication-key	265
	data-encapsulation	266
	default-peer	267
	disable (Protocols MSDP)	268
	export (Protocols MSDP)	269
	group (Protocols MSDP)	270
	hold-time (Protocols MSDP)	271
	import (Protocols MSDP)	272
	keep-alive (Protocols MSDP)	273
	local-address (Protocols MSDP)	274
	log-interval (Protocols MSDP)	275
	log-warning (Protocols MSDP)	276
	maximum (MSDP Active Source Messages)	277
	mode (Protocols MSDP)	278
	peer (Protocols MSDP)	279
	rib-group (Protocols MSDP)	280
	sa-hold-time (Protocols MSDP)	281
	source (Protocols MSDP)	282
	threshold (MSDP Active Source Messages)	283
	traceoptions (Protocols MSDP)	284
Chapter 17	Configuration Statements: PIM	287
	[edit protocols pim] Hierarchy Level	290
	accept-remote-source	294
	address (Anycast RPs)	295
	address (Bidirectional Rendezvous Points)	296
	address (Local RPs)	297
	address (Static RPs)	298
	algorithm	299
	anycast-pim	300
	assert-timeout	301
	authentication (Protocols PIM)	302
	auto-rp	303
	backoff-period	304
	bfd-liveness-detection (Protocols PIM)	305
	bidirectional (Interface)	306
	bidirectional (RP)	307
	bootstrap	308
	bootstrap-export	309

bootstrap-import	310
bootstrap-priority	311
dense-groups	312
detection-time (BFD for PIM)	313
df-election	314
disable (PIM Graceful Restart)	315
disable (PIM)	316
dr-election-on-p2p	317
dr-register-policy	317
embedded-rp	318
export (Protocols PIM Bootstrap)	319
export (Protocols PIM)	320
family (Bootstrap)	321
family (Protocols PIM)	322
family (Protocols PIM Interface)	323
family (Local RP)	324
graceful-restart (Protocols PIM)	325
group (RPF Selection)	326
group-ranges	327
group-rp-mapping	328
hello-interval (Protocols PIM)	329
hold-time (Protocols PIM)	330
idle-standby-path-switchover-delay	331
import (Protocols PIM Bootstrap)	332
import (Protocols PIM)	333
infinity	334
interface (Protocols PIM)	335
join-load-balance	337
join-prune-timeout	338
key-chain (Protocols PIM)	339
local	340
local-address (Protocols PIM)	341
log-interval (PIM Entries)	342
loose-check	343
mapping-agent-election	344
maximum (PIM Entries)	345
maximum-rps	346
minimum-interval (PIM BFD Liveness Detection)	347
minimum-interval (PIM BFD Transmit Interval)	348
minimum-receive-interval	349
mode (Protocols PIM)	350
multiplier	351
neighbor-policy	351
next-hop (PIM RPF Selection)	352
no-adaptation (PIM BFD Liveness Detection)	352
no-bidirectional-mode	353
no-dr-flood (PIM Snooping)	354
offer-period	355
override (PIM static RP)	356

	override-interval	357
	pim	358
	pim-snooping	363
	prefix-list (PIM RPF Selection)	364
	priority (Bootstrap)	365
	priority (PIM Interfaces)	366
	priority (PIM RPs)	367
	propagation-delay	368
	register-limit	369
	reset-tracking-bit	370
	restart-duration (Protocols PIM)	371
	rib-group (Protocols PIM)	372
	robustness-count	373
	rp	374
	rp-register-policy	376
	rp-set	377
	rpf-selection	378
	sglimit	379
	source (PIM RPF Selection)	380
	spt-threshold	381
	standby-path-creation-delay	382
	static (Protocols PIM)	383
	threshold (PIM BFD Detection Time)	384
	threshold (PIM BFD Transmit Interval)	385
	threshold (PIM Entries)	386
	traceoptions (Protocols PIM)	388
	traceoptions (PIM Snooping)	391
	transmit-interval (PIM BFD Liveness Detection)	392
	tunnel-devices (Tunnel-Capable PICs)	393
	version (BFD)	394
	version (PIM)	395
	vlan (PIM Snooping)	396
	vpn-group-address	396
	wildcard-source (PIM RPF Selection)	397
Chapter 18	Operational Commands: IGMP	399
	clear igmp statistics	400
	show igmp group	402
	show igmp interface	406
	show multicast pim-to-igmp-proxy	410
Chapter 19	Operational Commands: IGMP Snooping	413
	clear igmp snooping membership	414
	clear igmp snooping statistics	415
	show igmp snooping interface	416
	show igmp snooping membership	421
	show igmp snooping statistics	425

Chapter 20	Operational Commands: MLD	431
	clear mld membership	432
	clear mld statistics	433
	show mld group	434
	show mld interface	438
	show mld statistics	442
	show multicast pim-to-mld-proxy	445
Chapter 21	Operational Commands: MLD Snooping	447
	clear mld snooping membership	448
	clear mld snooping statistics	449
	show mld snooping interface	450
	show mld snooping membership	453
	show mld snooping statistics	456
	show route forwarding-table	459
	show multicast snooping route	467
	show route snooping	471
Chapter 22	Operational Commands: MSDP	475
	show msdp	476
	show msdp source	478
	show msdp source-active	480
	show msdp statistics	483
	show multicast usage	487
	show route table	490
Chapter 23	Operational Commands: PIM	505
	clear pim join	506
	clear pim join-distribution	508
	clear pim register	510
	clear pim statistics	512
	request pim multicast-tunnel rebalance	515
	show pim bidirectional df-election	516
	show pim bidirectional df-election interface	519
	show pim bootstrap	522
	show pim interfaces	524
	show pim join	527
	show pim neighbors	549
	show pim rps	553
	show pim source	560
	show pim statistics	563

List of Figures

Part 1	Overview	
Chapter 1	Understanding Multicast	3
	Figure 1: Multicast Terminology in an IP Network	6
	Figure 2: Converting MAC Addresses to Multicast Addresses	10
Part 2	Managing Group Membership	
Chapter 3	Managing Group Membership with MLD (IPv6)	43
	Figure 3: Routing Devices Start Up on a Subnet	44
	Figure 4: Querier Routing Device Is Determined	44
	Figure 5: General Query Message Is Issued	45
	Figure 6: Reports Are Received by the Querier Routing Device	45
	Figure 7: Host Has No Interested Receivers and Sends a Done Message to Routing Device	45
	Figure 8: Host Address Timer Expires and Address Is Removed from Multicast Address List	46
	Figure 9: Multicast Traffic Flow with MLD Snooping Enabled	47
	Figure 10: Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts	51
	Figure 11: Scenario 2: Switch Forwarding Multicast Traffic to Another Switch . . .	52
	Figure 12: Scenario 3: Switch Connected to Hosts Only (No MLD Querier)	53
	Figure 13: Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs	54
	Figure 14: MLD Snooping Topology Example	61
Part 3	Configuring Protocol Independent Multicast	
Chapter 6	Routing Content to Densely Clustered Receivers with PIM Dense Mode	93
	Figure 15: Multicast Traffic Flooded from the Source Using PIM Dense Mode . . .	94
	Figure 16: Prune Messages Sent Back to the Source to Stop Unwanted Multicast Traffic	95
Chapter 7	Routing Content to Larger, Sparser Groups with PIM Sparse Mode	99
	Figure 17: Extracting the Embedded RP IPv6 Address	104
Chapter 8	Rapidly Detecting Communication Failures with PIM and BFD Protocol	131
	Figure 18: BFD Liveness Detection for PIM IPv6 Topology	138

Part 5	Configuring Multicast VPNs	
Chapter 10	Configuring PIM Join Load Balancing	151
	Figure 19: PIM Join Load Balancing	153
Part 6	Configuring General Multicast Options	
Chapter 11	Enabling Multicast Between Layer 2 and Layer 3 Devices Using Snooping	159
	Figure 20: PIM Snooping for VPLS	161

List of Tables

	About the Documentation	xvii
	Table 1: Notice Icons	xix
	Table 2: Text and Syntax Conventions	xix
Part 1	Overview	
Chapter 1	Understanding Multicast	3
	Table 3: Multicast Routing Protocols Compared	13
Part 2	Managing Group Membership	
Chapter 2	IGMP	19
	Table 4: IGMP Event Messages	38
Chapter 3	Managing Group Membership with MLD (IPv6)	43
	Table 5: Supported Tracing Operations for MLD Snooping	67
Part 3	Configuring Protocol Independent Multicast	
Chapter 7	Routing Content to Larger, Sparser Groups with PIM Sparse Mode	99
	Table 6: Local RP and Auto-RP Message Types	100
	Table 7: PIM Join Filter Match Conditions	125
Part 7	Configuration Statements and Operational Commands	
Chapter 18	Operational Commands: IGMP	399
	Table 8: show igmp group Output Fields	402
	Table 9: show igmp interface Output Fields	406
	Table 10: show multicast pim-to-igmp-proxy Output Fields	410
Chapter 19	Operational Commands: IGMP Snooping	413
	Table 11: show igmp snooping interface Output Fields	416
	Table 12: show igmp snooping membership Output Fields	421
	Table 13: show igmp snooping statistics Output Fields	425
Chapter 20	Operational Commands: MLD	431
	Table 14: show mld group Output Fields	434
	Table 15: show mld interface Output Fields	438
	Table 16: show mld statistics Output Fields	442
	Table 17: show multicast pim-to-mld-proxy Output Fields	445
Chapter 21	Operational Commands: MLD Snooping	447
	Table 18: show mld snooping interface Output Fields	451

	Table 19: show mld snooping membership Output Fields	454
	Table 20: show mld statistics Output Fields	456
	Table 21: show route forwarding-table Output Fields	460
	Table 22: show multicast snooping route Output Fields	468
Chapter 22	Operational Commands: MSDP	475
	Table 23: show msdp Output Fields	476
	Table 24: show msdp source Output Fields	479
	Table 25: show msdp source-active Output Fields	481
	Table 26: show msdp statistics Output Fields	483
	Table 27: show multicast usage Output Fields	488
Chapter 23	Operational Commands: PIM	505
	Table 28: show pim bidirectional df-election Output Fields	516
	Table 29: show pim bidirectional df-election interface Output Fields	519
	Table 30: show pim bootstrap Output Fields	522
	Table 31: show pim interfaces Output Fields	524
	Table 32: show pim join Output Fields	529
	Table 33: show pim neighbors Output Fields	550
	Table 34: show pim rps Output Fields	554
	Table 35: show pim source Output Fields	561
	Table 36: show pim statistics Output Fields	564

About the Documentation

- Documentation and Release Notes on page xvii
- Supported Platforms on page xvii
- Using the Examples in This Manual on page xvii
- Documentation Conventions on page xix
- Documentation Feedback on page xxi
- Requesting Technical Support on page xxi

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 xix 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 xix 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.	<pre>user@host> show chassis alarms</pre> <p>No alarms currently active</p>
<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.	<p>Configure the machine's domain name:</p> <pre>[edit] root@# set system domain-name domain-name</pre>
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 <code>[edit protocols ospf area area-id]</code> 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 string2 string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
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 at the Juniper Networks Technical Documentation 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 <https://www.juniper.net/cgi-bin/docbugreport/>.
- 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>.

PART 1

Overview

- [Understanding Multicast on page 3](#)

CHAPTER 1

Understanding Multicast

- [Multicast Overview on page 3](#)
- [Supported IP Multicast Protocol Standards on page 15](#)

Multicast Overview

IP has three fundamental types of addresses: unicast, broadcast, and multicast. A *unicast address* is used to send a packet to a single destination. A *broadcast address* is used to send a datagram to an entire subnetwork. A *multicast address* is used to send a datagram to a set of hosts that can be on different subnetworks and that are configured as members of a multicast group.

A multicast datagram is delivered to destination group members with the same best-effort reliability as a standard unicast IP datagram. This means that multicast datagrams are not guaranteed to reach all members of a group or to arrive in the same order in which they were transmitted. The only difference between a multicast IP packet and a unicast IP packet is the presence of a group address in the IP header destination address field. Multicast addresses use the Class D address format.

Individual hosts can join or leave a multicast group at any time. There are no restrictions on the physical location or the number of members in a multicast group. A host can be a member of more than one multicast group at any time. A host does not have to belong to a group to send packets to members of a group.

Routing devices use a group membership protocol to learn about the presence of group members on directly attached subnetworks. When a host joins a multicast group, it transmits a group membership protocol message for the group or groups that it wants to receive and sets its IP process and network interface card to receive frames addressed to the multicast group.

Comparing Multicast to Unicast

The Junos[®] operating system (Junos OS) routing protocol process supports a wide variety of routing protocols. These routing protocols carry network information among routing devices not only for *unicast* traffic streams sent between one pair of clients and servers, but also for *multicast* traffic streams containing video, audio, or both, between a single server source and many client receivers. The routing protocols used for multicast differ in many key ways from unicast routing protocols.

Information is delivered over a network by three basic methods: unicast, broadcast, and multicast.

The differences among unicast, broadcast, and multicast can be summarized as follows:

- Unicast: One-to-one, from one source to one destination.
- Broadcast: One-to-all, from one source to all possible destinations.
- Multicast: One-to-many, from one source to multiple destinations expressing an interest in receiving the traffic.



NOTE: This list does not include a special category for many-to-many applications, such as online gaming or videoconferencing, where there are many sources for the same receiver and where receivers often double as sources. Many-to-many is a service model that repeatedly employs one-to-many multicast and therefore requires no unique protocol. The original multicast specification, RFC 1112, supports both the any-source multicast (ASM) many-to-many model and the source-specific multicast (SSM) one-to-many model.

With unicast traffic, many streams of IP packets that travel across networks flow from a single source, such as a website server, to a single destination such as a client PC. Unicast traffic is still the most common form of information transfer on networks.

Broadcast traffic flows from a single source to all possible destinations reachable on the network, which is usually a LAN. Broadcasting is the easiest way to make sure traffic reaches its destinations.

Television networks use broadcasting to distribute video and audio. Even if the television network is a cable television (CATV) system, the source signal reaches all possible destinations, which is the main reason that some channels' content is scrambled. Broadcasting is not feasible on the Internet because of the enormous amount of unnecessary information that would constantly arrive at each end user's device, the complexities and impact of scrambling, and related privacy issues.

Multicast traffic lies between the extremes of unicast (one source, one destination) and broadcast (one source, all destinations). Multicast is a "one source, many destinations" method of traffic distribution, meaning only the destinations that explicitly indicate their need to receive the information from a particular source receive the traffic stream.

On an IP network, because destinations (clients) do not often communicate directly with sources (servers), the routing devices between source and destination must be able to determine the topology of the network from the unicast or multicast perspective to avoid routing traffic haphazardly. Multicast routing devices replicate packets received on one input interface and send the copies out on multiple output interfaces.

In IP multicast, the source and destination are almost always hosts and not routing devices. Multicast routing devices distribute the multicast traffic across the network from source to destinations. The multicast routing device must find multicast sources on the

network, send out copies of packets on several interfaces, prevent routing loops, connect interested destinations with the proper source, and keep the flow of unwanted packets to a minimum. Standard multicast routing protocols provide most of these capabilities, but some router architectures cannot send multiple copies of packets and so do not support multicasting directly.

IP Multicast Uses

Multicast allows an IP network to support more than just the unicast model of data delivery that prevailed in the early stages of the Internet. Multicast, originally defined as a host extension in RFC 1112 in 1989, provides an efficient method for delivering traffic flows that can be characterized as one-to-many or many-to-many.

Unicast traffic is not strictly limited to data applications. Telephone conversations, wireless or not, contain digital audio samples and might contain digital photographs or even video and still flow from a single source to a single destination. In the same way, multicast traffic is not strictly limited to multimedia applications. In some data applications, the flow of traffic is from a single source to many destinations that require the packets, as in a news or stock ticker service delivered to many PCs. For this reason, the term *receiver* is preferred to *listener* for multicast destinations, although both terms are common.

Network applications that can function with unicast but are better suited for multicast include collaborative groupware, teleconferencing, periodic or “push” data delivery (stock quotes, sports scores, magazines, newspapers, and advertisements), server or website replication, and distributed interactive simulation (DIS) such as war simulations or virtual reality. Any IP network concerned with reducing network resource overhead for one-to-many or many-to-many data or multimedia applications with multiple receivers benefits from multicast.

If unicast were employed by radio or news ticker services, each radio or PC would have to have a separate traffic session for each listener or viewer at a PC (this is actually the method for some Web-based services). The processing load and bandwidth consumed by the server would increase linearly as more people “tune in” to the server. This is extremely inefficient when dealing with the global scale of the Internet. Unicast places the burden of packet duplication on the server and consumes more and more backbone bandwidth as the number of users grows.

If broadcast were employed instead, the source could generate a single IP packet stream using a broadcast destination address. Although broadcast eliminates the server packet duplication issue, this is not a good solution for IP because IP broadcasts can be sent only to a single subnetwork, and IP routing devices normally isolate IP subnetworks on separate interfaces. Even if an IP packet stream could be addressed to literally go everywhere, and there were no need to “tune” to any source at all, broadcast would be extremely inefficient because of the bandwidth strain and need for uninterested hosts to discard large numbers of packets. Broadcast places the burden of packet rejection on each host and consumes the maximum amount of backbone bandwidth.

For radio station or news ticker traffic, multicast provides the most efficient and effective outcome, with none of the drawbacks and all of the advantages of the other methods. A single source of multicast packets finds its way to every *interested* receiver. As with

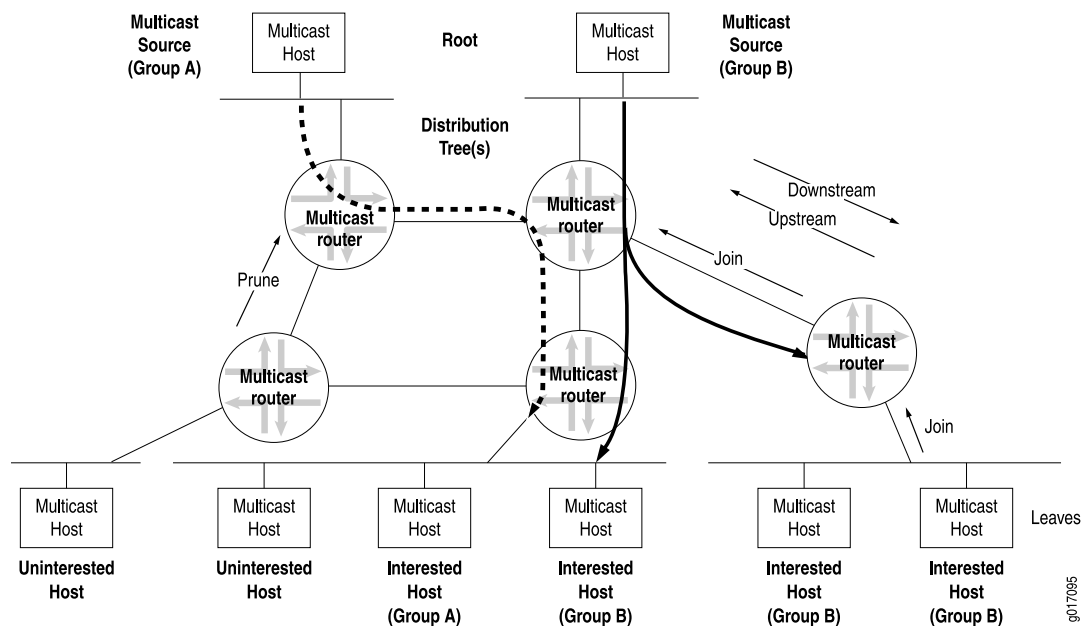
broadcast, the transmitting host generates only a single stream of IP packets, so the load remains constant whether there is one receiver or one million. The network routing devices replicate the packets and deliver the packets to the proper receivers, but only the replication role is a new one for routing devices. The links leading to subnets consisting of entirely uninterested receivers carry no multicast traffic. Multicast minimizes the burden placed on sender, network, and receiver.

IP Multicast Terminology

Multicast has its own particular set of terms and acronyms that apply to IP multicast routing devices and networks. [Figure 1 on page 6](#) depicts some of the terms commonly used in an IP multicast network.

In a multicast network, the key component is the *routing device*, which is able to replicate packets and is therefore multicast-capable. The routing devices in the IP multicast network, which has exactly the same topology as the unicast network it is based on, use a *multicast routing protocol* to build a *distribution tree* that connects receivers (preferred to the multimedia implications of listeners, but listeners is also used) to *sources*. In multicast terminology, the distribution tree is *rooted at the source* (the root of the distribution tree is the source). The interface on the routing device leading toward the source is the *upstream* interface, although the less precise terms *incoming* or *inbound* interface are used as well. To keep bandwidth use to a minimum, it is best for only one upstream interface on the routing device to receive multicast packets. The interface on the routing device leading toward the receivers is the *downstream* interface, although the less precise terms *outgoing* or *outbound* interface are used as well. There can be 0 to $N-1$ downstream interfaces on a routing device, where N is the number of logical interfaces on the routing device. To prevent looping, the upstream interface must never receive copies of downstream multicast packets.

Figure 1: Multicast Terminology in an IP Network



Routing loops are disastrous in multicast networks because of the risk of repeatedly replicated packets. One of the complexities of modern multicast routing protocols is the need to avoid routing loops, packet by packet, much more rigorously than in unicast routing protocols. Three multicast strategies—reverse-path forwarding (RPF), shortest-path tree (SPT), and administrative scoping—help prevent routing loops by defining routing paths in different ways.

Reverse-Path Forwarding for Loop Prevention

The routing device's multicast forwarding state runs more logically based on the reverse path, from the receiver back to the root of the distribution tree. In RPF, every multicast packet received must pass an RPF check before it can be replicated or forwarded on any interface. When it receives a multicast packet on an interface, the routing device verifies that the *source* address in the multicast IP packet is the *destination* address for a unicast IP packet back to the source.

If the outgoing interface found in the unicast routing table is the same interface that the multicast packet was received on, the packet passes the RPF check. Multicast packets that fail the RPF check are dropped, because the incoming interface is not on the shortest path back to the source. Routing devices can build and maintain separate tables for RPF purposes.

Shortest-Path Tree for Loop Prevention

The distribution tree used for multicast is rooted at the source and is the shortest-path tree (SPT), but this path can be long if the source is at the periphery of the network. Providing a *shared tree* on the backbone as the distribution tree locates the multicast source more centrally in the network. Shared distribution trees with roots in the core network are created and maintained by a multicast routing device operating as a rendezvous point (RP), a feature of sparse mode multicast protocols.

Administrative Scoping for Loop Prevention

Scoping limits the routing devices and interfaces that can forward a multicast packet. Multicast scoping is *administrative* in the sense that a range of multicast addresses is reserved for scoping purposes, as described in RFC 2365, *Administratively Scoped IP Multicast*. Routing devices at the boundary must filter multicast packets and ensure that packets do not stray beyond the established limit.

Multicast Leaf and Branch Terminology

Each subnetwork with hosts on the routing device that has at least one interested receiver is a *leaf* on the distribution tree. Routing devices can have multiple leaves on different interfaces and must send a copy of the IP multicast packet out on each interface with a leaf. When a new leaf subnetwork is added to the tree (that is, the interface to the host subnetwork previously received no copies of the multicast packets), a new *branch* is built, the leaf is joined to the tree, and replicated packets are sent out on the interface. The number of leaves on a particular interface does not affect the routing device. The action is the same for one leaf or a hundred.



NOTE: On Juniper Networks security devices, if the maximum number of leaves on a multicast distribution tree is exceeded, multicast sessions are created up to the maximum number of leaves, and any multicast sessions that exceed the maximum number of leaves are ignored. The maximum number of leaves on a multicast distribution tree is device specific.

When a branch contains no leaves because there are no interested hosts on the routing device interface leading to that IP subnetwork, the branch is *pruned* from the distribution tree, and no multicast packets are sent out that interface. Packets are replicated and sent out multiple interfaces only where the distribution tree branches at a routing device, and no link ever carries a duplicate flow of packets.

Collections of hosts all receiving the same stream of IP packets, usually from the same multicast source, are called *groups*. In IP multicast networks, traffic is delivered to multicast groups based on an IP multicast address, or *group address*. The groups determine the location of the leaves, and the leaves determine the branches on the multicast network.

IP Multicast Addressing

Multicast uses the Class D IP address range (224.0.0.0 through 239.255.255.255). Class D addresses are commonly referred to as *multicast addresses* because the entire classful address concept is obsolete. Multicast addresses can never appear as the source address in an IP packet and can only be the destination of a packet.

Multicast addresses usually have a prefix length of /32, although other prefix lengths are allowed. Multicast addresses represent logical groupings of receivers and not physical collections of devices. Blocks of multicast addresses can still be described in terms of prefix length in traditional notation, but only for convenience. For example, the multicast address range from 232.0.0.0 through 232.255.255.255 can be written as 232.0.0.0/8 or 232/8.

Internet service providers (ISPs) do not typically allocate multicast addresses to their customers because multicast addresses relate to content, not to physical devices. Receivers are not assigned their own multicast addresses, but need to know the multicast address of the content. Sources need to be assigned multicast addresses only to produce the content, not to identify their place in the network. Every source and receiver still needs an ordinary, unicast IP address.

Multicast addressing most often references the receivers, and the source of multicast content is usually not even a member of the multicast group for which it produces content. If the source needs to monitor the packets it produces, monitoring can be done locally, and there is no need to make the packets traverse the network.

Many applications have been assigned a range of multicast addresses for their own use. These applications assign multicast addresses to sessions created by that application. You do not usually need to statically assign a multicast address, but you can do so.

Multicast Addresses

Multicast host group addresses are defined to be the IP addresses whose high-order four bits are 1110, giving an address range from 224.0.0.0 through 239.255.255.255, or simply 224.0.0.0/4. (These addresses also are referred to as Class D addresses.)

The Internet Assigned Numbers Authority (IANA) maintains a list of registered IP multicast groups. The base address 224.0.0.0 is reserved and cannot be assigned to any group. The block of multicast addresses from 224.0.0.1 through 224.0.0.255 is reserved for local wire use. Groups in this range are assigned for various uses, including routing protocols and local discovery mechanisms.

The range from 239.0.0.0 through 239.255.255.255 is reserved for administratively scoped addresses. Because packets addressed to administratively scoped multicast addresses do not cross configured administrative boundaries, and because administratively scoped multicast addresses are locally assigned, these addresses do not need to be unique across administrative boundaries.

Layer 2 Frames and IPv4 Multicast Addresses

Multicasting on a LAN is a good place to start an investigation of multicasting at Layer 2. At Layer 2, multicast deals with media access control (MAC) frames and addresses instead of IPv4 or IPv6 packets and addresses. Consider a single LAN, without routing devices, with a multicast source sending to a certain group. The rest of the hosts are receivers interested in the multicast group's content. So the multicast source host generates packets with its unicast IP address as the source, and the multicast group address as the destination.

Which MAC addresses are used on the frame containing this packet? The packet source address—the unicast IP address of the host originating the multicast content—translates easily and directly to the MAC address of the source. But what about the packet's destination address? This is the IP multicast group address. Which destination MAC address for the frame corresponds to the packet's multicast group address?

One option is for LANs simply to use the LAN broadcast MAC address, which guarantees that the frame is processed by every station on the LAN. However, this procedure defeats the whole purpose of multicast, which is to limit the circulation of packets and frames to interested hosts. Also, hosts might have access to many multicast groups, which multiplies the amount of traffic to noninterested destinations. Broadcasting frames at the LAN level to support multicast groups makes no sense.

However, there is an easy way to effectively use Layer 2 frames for multicast purposes. The MAC address has a bit that is set to 0 for unicast (the LAN term is *individual address*) and set to 1 to indicate that this is a multicast address. Some of these addresses are reserved for multicast groups of specific vendors or MAC-level protocols. Internet multicast applications use the range 0x01-00-5E-00-00-00 to 0x01-00-5E-FF-FF-FF. Multicast receivers (hosts running TCP/IP) listen for frames with one of these addresses when the application joins a multicast group. The host stops listening when the application terminates or the host leaves the group at the packet layer (Layer 3).

This means that 3 bytes, or 24 bits, are available to map IPv4 multicast addresses at Layer 3 to MAC multicast addresses at Layer 2. However, all IPv4 addresses, including multicast addresses, are 32 bits long, leaving 8 IP address bits left over. Which method of mapping IPv4 multicast addresses to MAC multicast addresses minimizes the chance of “collisions” (that is, two different IP multicast groups at the packet layer mapping to the same MAC multicast address at the frame layer)?

First, it is important to realize that all IPv4 multicast addresses begin with the same 4 bits (1110), so there are really only 4 bits of concern, not 8. A LAN must not drop the last bits of the IPv4 address because these are almost guaranteed to be host bits, depending on the subnet mask. But the high-order bits, the leftmost address bits, are almost always network bits, and there is only one LAN (for now).

One other bit of the remaining 24 MAC address bits is reserved (an initial 0 indicates an Internet multicast address), so the 5 bits following the initial 1110 in the IPv4 address are dropped. The 23 remaining bits are mapped, one for one, into the last 23 bits of the MAC address. An example of this process is shown in [Figure 2 on page 10](#).

Figure 2: Converting MAC Addresses to Multicast Addresses

1	IPv4 header multicast destination address	232.	224.	202.	181
	Written in hexadecimal	E8	E0	CA	B5
	Written in binary	1110 1000 1	110 0000	1100 1010	1011 0101
2	Ignore the first 9 bits and copy the remaining 23 bits	X	110 0000	1100 1010	1011 0101
3	First bit X = 0 for Internet; X = 1 for other	0	110 0000	1100 1010	1011 0101
4	Written in hexadecimal		60	CA	B5
5	MAC address in hexadecimal	01 : 00 : 5E : E0 : CA : B5			
6	Drop last 24 bits	01 : 00 : 5E :			
7	Copy the multicast bits	01 : 00 : 5E : 60 : CA : B5			
8	MAC frame destination address 01:00:5E:60:CA:B5 corresponds to multicast IPv4 address 232.224.202.181				

Note that this process means that there are 32 (2^5) IPv4 multicast addresses that could map to the same MAC multicast addresses. For example, multicast IPv4 addresses 224.8.7.6 and 229.136.7.6 translate to the same MAC address (0x01-00-5E-08-07-06). This is a real concern, and because the host could be interested in frames sent to both of the those multicast groups, the IP software must reject one or the other.



NOTE: This “collision” problem does not exist in IPv6 because of the way IPv6 handles multicast groups, but it is always a concern in IPv4. The procedure for placing IPv6 multicast packets inside multicast frames is nearly identical to that for IPv4, except for the MAC destination address 0x3333 prefix (and the lack of “collisions”).

Once the MAC address for the multicast group is determined, the host's operating system essentially orders the LAN interface card to join or leave the multicast group. Once joined to a multicast group, the host accepts frames sent to the multicast address as well as the host's unicast address and ignores other multicast group's frames. It is possible for a host to join and receive multicast content from more than one group at the same time, of course.

Multicast Interface Lists

To avoid multicast routing loops, every multicast routing device must always be aware of the interface that leads to the source of that multicast group content by the shortest path. This is the upstream (incoming) interface, and packets are never to be forwarded back toward a multicast source. All other interfaces are potential downstream (outgoing) interfaces, depending on the number of branches on the distribution tree.

Routing devices closely monitor the status of the incoming and outgoing interfaces, a process that determines the *multicast forwarding state*. A routing device with a multicast forwarding state for a particular multicast group is essentially “turned on” for that group's content. Interfaces on the routing device's outgoing interface list send copies of the group's packets received on the incoming interface list for that group. The incoming and outgoing interface lists might be different for different multicast groups.

The multicast forwarding state in a routing device is usually written in either (S,G) or (*G) notation. These are pronounced “ess comma gee” and “star comma gee,” respectively. In (S,G), the S refers to the unicast IP address of the source for the multicast traffic, and the G refers to the particular multicast group IP address for which S is the source. All multicast packets sent from this source have S as the source address and G as the destination address.

The asterisk (*) in the (*G) notation is a wildcard indicating that the state applies to any multicast application source sending to group G. So, if two sources are originating exactly the same content for multicast group 224.1.1.2, a routing device could use (*224.1.1.2) to represent the state of a routing device forwarding traffic from both sources to the group.

Multicast Routing Protocols

Multicast routing protocols enable a collection of multicast routing devices to build (join) distribution trees when a host on a directly attached subnet, typically a LAN, wants to receive traffic from a certain multicast group, prune branches, locate sources and groups, and prevent routing loops.

There are several multicast routing protocols:

- Distance Vector Multicast Routing Protocol (DVMRP)—The first of the multicast routing protocols and hampered by a number of limitations that make this method unattractive for large-scale Internet use. DVMRP is a dense-mode-only protocol, and uses the flood-and-prune or implicit join method to deliver traffic everywhere and then determine where the uninterested receivers are. DVMRP uses source-based distribution trees in the form (S,G), and builds its own multicast routing tables for RPF checks.
- Multicast OSPF (MOSPF)—Extends OSPF for multicast use, but only for dense mode. However, MOSPF has an explicit join message, so routing devices do not have to flood

their entire domain with multicast traffic from every source. MOSPF uses source-based distribution trees in the form (S,G).

- *Bidirectional PIM mode*—A variation of PIM. Bidirectional PIM builds bidirectional shared trees that are rooted at a rendezvous point (RP) address. Bidirectional traffic does not switch to shortest path trees as in PIM-SM and is therefore optimized for routing state size instead of path length. This means that the end-to-end latency might be longer compared to PIM sparse mode. Bidirectional PIM routes are always wildcard-source (*G) routes. The protocol eliminates the need for (S,G) routes and data-triggered events. The bidirectional (*G) group trees carry traffic both upstream from senders toward the RP, and downstream from the RP to receivers. As a consequence, the strict reverse path forwarding (RPF)-based rules found in other PIM modes do not apply to bidirectional PIM. Instead, bidirectional PIM (*G) routes forward traffic from all sources and the RP. Bidirectional PIM routing devices must have the ability to accept traffic on many potential incoming interfaces. Bidirectional PIM scales well because it needs no source-specific (S,G) state. Bidirectional PIM is recommended in deployments with many dispersed sources and many dispersed receivers.
- *PIM dense mode*—In this mode of PIM, the assumption is that almost all possible subnets have at least one receiver wanting to receive the multicast traffic from a source, so the network is *flooded* with traffic on all possible branches, then pruned back when branches do not express an interest in receiving the packets, explicitly (by message) or implicitly (time-out silence). This is the *dense mode* of multicast operation. LANs are appropriate networks for dense-mode operation. Some multicast routing protocols, especially older ones, support only dense-mode operation, which makes them inappropriate for use on the Internet. In contrast to DVMRP and MOSPF, PIM dense mode allows a routing device to use any unicast routing protocol and performs RPF checks using the unicast routing table. PIM dense mode has an implicit join message, so routing devices use the flood-and-prune method to deliver traffic everywhere and then determine where the uninterested receivers are. PIM dense mode uses source-based distribution trees in the form (S,G), as do all dense-mode protocols. PIM also supports sparse-dense mode, with mixed sparse and dense groups, but there is no special notation for that operational mode. If *sparse-dense mode* is supported, the multicast routing protocol allows some multicast groups to be sparse and other groups to be dense.
- *PIM sparse mode*—In this mode of PIM, the assumption is that very few of the possible receivers want packets from each source, so the network establishes and sends packets only on branches that have at least one leaf indicating (by message) an interest in the traffic. This multicast protocol allows a routing device to use any unicast routing protocol and performs reverse-path forwarding (RPF) checks using the unicast routing table. PIM sparse mode has an *explicit* join message, so routing devices determine where the interested receivers are and send join messages upstream to their neighbors, building trees from receivers to the rendezvous point (RP). PIM sparse mode uses an RP routing device as the initial source of multicast group traffic and therefore builds distribution trees in the form (*G), as do all sparse-mode protocols. PIM sparse mode migrates to an (S,G) source-based tree if that path is shorter than through the RP for a particular multicast group's traffic. WANs are appropriate networks for sparse-mode operation, and indeed a common multicast guideline is not to run dense mode on a WAN under any circumstances.

- Core Based Trees (CBT)—Shares all of the characteristics of PIM sparse mode (sparse mode, explicit join, and shared (*G) trees), but is said to be more efficient at finding sources than PIM sparse mode. CBT is rarely encountered outside academic discussions. There are no large-scale deployments of CBT, commercial or otherwise.
- PIM source-specific multicast (SSM)—Enhancement to PIM sparse mode that allows a client to receive multicast traffic directly from the source, without the help of an RP. Used with IGMPv3 to create a shortest-path tree between receiver and source.
- IGMPv1—The original protocol defined in RFC 1112, *Host Extensions for IP Multicasting*. IGMPv1 sends an explicit join message to the routing device, but uses a timeout to determine when hosts leave a group. Three versions of the Internet Group Management Protocol (IGMP) run between receiver hosts and routing devices.
- IGMPv2—Defined in RFC 2236, *Internet Group Management Protocol, Version 2*. Among other features, IGMPv2 adds an explicit leave message to the join message.
- IGMPv3—Defined in RFC 3376, *Internet Group Management Protocol, Version 3*. Among other features, IGMPv3 optimizes support for a single source of content for a multicast group, or source-specific multicast (SSM). Used with PIM SSM to create a shortest-path tree between receiver and source.
- Bootstrap Router (BSR) and Auto-Rendezvous Point (RP)—Allow sparse-mode routing protocols to find RPs within the routing domain (autonomous system, or AS). RP addresses can also be statically configured.
- Multicast Source Discovery Protocol (MSDP)—Allows groups located in one multicast routing domain to find RPs in other routing domains. MSDP is not used on an RP if all receivers and sources are located in the same routing domain. Typically runs on the same routing device as PIM sparse mode RP. Not appropriate if all receivers and sources are located in the same routing domain.
- Session Announcement Protocol (SAP) and Session Description Protocol (SDP)—Display multicast session names and correlate the names with multicast traffic. SDP is a session directory protocol that advertises multimedia conference sessions and communicates setup information to participants who want to join the session. A client commonly uses SDP to announce a conference session by periodically multicasting an announcement packet to a well-known multicast address and port using SAP.
- Pragmatic General Multicast (PGM)—Special protocol layer for multicast traffic that can be used between the IP layer and the multicast application to add reliability to multicast traffic. PGM allows a receiver to detect missing information in all cases and request replacement information if the receiver application requires it.

The differences among the multicast routing protocols are summarized in [Table 3 on page 13](#).

Table 3: Multicast Routing Protocols Compared

Multicast Routing Protocol	Dense Mode	Sparse Mode	Implicit Join	Explicit Join	(S,G) SBT	(*G) Shared Tree
DVMRP	Yes	No	Yes	No	Yes	No

Table 3: Multicast Routing Protocols Compared (*continued*)

Multicast Routing Protocol	Dense Mode	Sparse Mode	Implicit Join	Explicit Join	(S,G) SBT	(*G) Shared Tree
MOSPF	Yes	No	No	Yes	Yes	No
PIM dense mode	Yes	No	Yes	No	Yes	No
PIM sparse mode	No	Yes	No	Yes	Yes, maybe	Yes, initially
Bidirectional PIM	No	No	No	Yes	No	Yes
CBT	No	Yes	No	Yes	No	Yes
SSM	No	Yes	No	Yes	Yes, maybe	Yes, initially
IGMPv1	No	Yes	No	Yes	Yes, maybe	Yes, initially
IGMPv2	No	Yes	No	Yes	Yes, maybe	Yes, initially
IGMPv3	No	Yes	No	Yes	Yes, maybe	Yes, initially
BSR and Auto-RP	No	Yes	No	Yes	Yes, maybe	Yes, initially
MSDP	No	Yes	No	Yes	Yes, maybe	Yes, initially

It is important to realize that retransmissions due to a high bit-error rate on a link or overloaded routing device can make multicast as inefficient as repeated unicast. Therefore, there is a trade-off in many multicast applications regarding the session support provided by the Transmission Control Protocol (TCP) (but TCP always resends missing segments), or the simple drop-and-continue strategy of the User Datagram Protocol (UDP) datagram service (but reordering can become an issue). Modern multicast uses UDP almost exclusively.

T Series Router Multicast Performance

The Juniper Networks T Series Core Routers handle extreme multicast packet replication requirements with a minimum of router load. Each memory component replicates a multicast packet twice at most. Even in the worst-case scenario involving maximum fan-out, when 1 input port and 63 output ports need a copy of the packet, the T Series routing platform copies a multicast packet only six times. Most multicast distribution trees are much sparser, so in many cases only two or three replications are necessary. In no case does the T Series architecture have an impact on multicast performance, even with the largest multicast fan-out requirements.

Supported IP Multicast Protocol Standards

Junos OS substantially supports the following RFCs and Internet drafts, which define standards for IP multicast protocols, including the Distance Vector Multicast Routing Protocol (DVMRP), Internet Group Management Protocol (IGMP), Multicast Listener Discovery (MLD), Multicast Source Discovery Protocol (MSDP), Pragmatic General Multicast (PGM), Protocol Independent Multicast (PIM), Session Announcement Protocol (SAP), and Session Description Protocol (SDP).

- RFC 1112, *Host Extensions for IP Multicasting* (defines IGMP Version 1)
- RFC 2236, *Internet Group Management Protocol, Version 2*
- RFC 2327, *SDP: Session Description Protocol*
- RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*
- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 3031, *Multiprotocol Label Switching Architecture*
- RFC 3376, *Internet Group Management Protocol, Version 3*
- RFC 3590, *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*
- RFC 4601, *Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised)*
- RFC 4604, *Using IGMPv3 and MLDv2 for Source-Specific Multicast*
- RFC 4607, *Source-Specific Multicast for IP*
- RFC 4610, *Anycast-RP Using Protocol Independent Multicast (PIM)*
- RFC 5015, *Bidirectional Protocol Independent Multicast (BIDIR-PIM)*
- RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*

The scoping mechanism is not supported.

- RFC 6513, *Multicast in MPLS/BGP IP VPNs*
- RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs*
- Internet draft draft-raggarwa-l3vpn-bgp-mvpn-extranet-08.txt, *Extranet in BGP Multicast VPN (MVPN)*
- Internet draft draft-rosen-l3vpn-spmsi-joins-mldp-03.txt, *MVPN: S-PMSI Join Extensions for mLDP-Created Tunnels*

The following RFCs and Internet drafts do not define standards, but provide information about multicast protocols and related technologies. The IETF classifies them variously as “Best Current Practice,” “Experimental,” or “Informational.”

- RFC 1075, *Distance Vector Multicast Routing Protocol*
- RFC 2362, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*
- RFC 2365, *Administratively Scoped IP Multicast*

- RFC 2547, *BGP/MPLS VPNs*
 - RFC 2974, *Session Announcement Protocol*
 - RFC 3208, *PGM Reliable Transport Protocol Specification*
 - RFC 3446, *Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*
 - RFC 3569, *An Overview of Source-Specific Multicast (SSM)*
 - RFC 3618, *Multicast Source Discovery Protocol (MSDP)*
 - RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
 - RFC 3973, *Protocol Independent Multicast – Dense Mode (PIM-DM): Protocol Specification (Revised)*
 - RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
 - Internet draft draft-ietf-idmr-dvmrp-v3-11.txt, *Distance Vector Multicast Routing Protocol*
 - Internet draft draft-ietf-mboned-ssm232-08.txt, *Source-Specific Protocol Independent Multicast in 232/8*
 - Internet draft draft-ietf-mmusic-sap-00.txt, *SAP: Session Announcement Protocol*
 - Internet draft draft-rosen-vpn-mcast-07.txt, *Multicast in MPLS/BGP VPNs*
- Only section 7, “Data MDT: Optimizing flooding,” is supported.

**Related
Documentation**

- *Accessing Standards Documents on the Internet*

PART 2

Managing Group Membership

- [IGMP on page 19](#)
- [Managing Group Membership with MLD \(IPv6\) on page 43](#)

CHAPTER 2

IGMP

- [Configuring IGMP on page 19](#)

Configuring IGMP

- [Understanding Group Membership Protocols on page 19](#)
- [Understanding IGMP on page 21](#)
- [Configuring IGMP on page 23](#)
- [Enabling IGMP on page 24](#)
- [Modifying the IGMP Host-Query Message Interval on page 25](#)
- [Modifying the IGMP Query Response Interval on page 26](#)
- [Specifying Immediate-Leave Host Removal for IGMP on page 26](#)
- [Filtering Unwanted IGMP Reports at the IGMP Interface Level on page 27](#)
- [Accepting IGMP Messages from Remote Subnetworks on page 28](#)
- [Modifying the IGMP Last-Member Query Interval on page 29](#)
- [Modifying the IGMP Robustness Variable on page 29](#)
- [Limiting the Maximum IGMP Message Rate on page 30](#)
- [Changing the IGMP Version on page 31](#)
- [Enabling IGMP Static Group Membership on page 31](#)
- [Recording IGMP Join and Leave Events on page 37](#)
- [Limiting the Number of IGMP Multicast Group Joins on Logical Interfaces on page 39](#)
- [Tracing IGMP Protocol Traffic on page 40](#)
- [Disabling IGMP on page 42](#)
- [IGMP and Nonstop Active Routing on page 42](#)

Understanding Group Membership Protocols

There is a big difference between the multicast protocols used between host and router and between the multicast routers themselves. Hosts on a given subnetwork need to inform their router only whether or not they are interested in receiving packets from a certain multicast group. The source host needs to inform its routers only that it is the source of traffic for a particular multicast group. In other words, no detailed knowledge of the distribution tree is needed by any hosts; only a group membership protocol is

needed to inform routers of their participation in a multicast group. Between adjacent routers, on the other hand, the multicast routing protocols must avoid loops as they build a detailed sense of the network topology and distribution tree from source to leaf. So, different multicast protocols are used for the host-router portion and the router-router portion of the multicast network.

Multicast group membership protocols enable a router to detect when a host on a directly attached subnet, typically a LAN, wants to receive traffic from a certain multicast group. Even if more than one host on the LAN wants to receive traffic for that multicast group, the router sends only one copy of each packet for that multicast group out on that interface, because of the inherent broadcast nature of LANs. When the multicast group membership protocol informs the router that there are no interested hosts on the subnet, the packets are withheld and that leaf is pruned from the distribution tree.

The Internet Group Management Protocol (IGMP) and the Multicast Listener Discovery (MLD) Protocol are the standard IP multicast group membership protocols: IGMP and MLD have several versions that are supported by hosts and routers:

- IGMPv1—The original protocol defined in RFC 1112. An explicit join message is sent to the router, but a timeout is used to determine when hosts leave a group. This process wastes processing cycles on the router, especially on older or smaller routers.
- IGMPv2—Defined in RFC 2236. Among other features, IGMPv2 adds an explicit leave message to the join message so that routers can more easily determine when a group has no interested listeners on a LAN.
- IGMPv3—Defined in RFC 3376. Among other features, IGMPv3 optimizes support for a single source of content for a multicast group, or *source-specific multicast (SSM)*.
- MLDv1—Defined in RFC 2710. MLDv1 is similar to IGMPv2.
- MLDv2—Defined in RFC 3810. MLDv2 similar to IGMPv3.

The various versions of IGMP and MLD are backward compatible. It is common for a router to run multiple versions of IGMP and MLD on LAN interfaces. Backward compatibility is achieved by dropping back to the most basic of all versions run on a LAN. For example, if one host is running IGMPv1, any router attached to the LAN running IGMPv2 can drop back to IGMPv1 operation, effectively eliminating the IGMPv2 advantages. Running multiple IGMP versions ensures that both IGMPv1 and IGMPv2 hosts find peers for their versions on the router.



CAUTION: On MX Series platforms, IGMPv2 and IGMPv3 cannot be configured together on the same interface. Configuring both together causes unexpected behavior in multicast traffic forwarding.

Understanding IGMP

The IPv4 address scheme assigns class D addresses for IP multicast. IGMP is the protocol that uses these addresses, which can be in the range 224.0.0.0 to 239.255.255.255. The following addresses have specific functions or are unavailable:

- 224.0.0.0 is reserved—you cannot assign it to a group.
- 224.0.0.1 is the all-hosts address—a packet sent to this address reaches all hosts on a subnet.
- 224.0.0.2 is the all-routers address—a packet sent to this address reaches all routers on a subnet.

This implementation of IGMP complies with IGMP versions 1, 2, and 3. IGMPv3 supports source-specific join and leave messages and is backward compatible with IGMPv1 and IGMPv2.

IGMPv2 mode interfaces exchange the following types of messages between routers and hosts:

- Group membership queries
- Group membership reports
- Leave group membership messages

IGMPv3 mode interfaces exchange the following types of messages with IGMPv3 hosts:

- Group membership queries
- IGMPv3 group membership reports

IGMP manages the membership of hosts and routers in multicast groups. IP hosts use IGMP to report their multicast group memberships to any immediately neighboring multicast routers. Multicast routers use IGMP to learn, for each of their attached physical networks, which groups have members.

A router receives explicit join and prune messages from those neighboring routers that have downstream group members. When PIM is the multicast protocol in use, IGMP begins the process as follows:

1. To join a multicast group, G, a host conveys its membership information through IGMP.
2. The router then forwards data packets addressed to a multicast group G to only those interfaces on which explicit join messages have been received.
3. A designated router (DR) sends periodic join and prune messages toward a group-specific rendezvous point (RP) for each group for which it has active members. One or more routers are automatically or statically designated as the RP, and all routers must explicitly join through the RP.
4. Each router along the path toward the RP builds a wild card (any-source) state for the group and sends join and prune messages toward the RP.

The term *route entry* is used to refer to the state maintained in a router to represent the distribution tree.

A route entry can include such fields as:

- source address
- group address
- incoming interface from which packets are accepted
- list of outgoing interfaces to which packets are sent
- timers
- flag bits

The wild card route entry's incoming interface points toward the RP.

The outgoing interfaces point to the neighboring downstream routers that have sent join and prune messages toward the RP as well as the directly connected hosts that have requested membership to group G.

5. This state creates a shared, RP-centered, distribution tree that reaches all group members.

IGMP is also used as the transport for several related multicast protocols (for example, Distance Vector Multicast Routing Protocol [DVMRP] and Protocol Independent Multicast version 1 [PIMv1]).

IGMP is an integral part of IP and must be enabled on all routers and hosts that need to receive IP multicast traffic.

For each attached network, a multicast router can be either a querier or a nonquerier. The querier router periodically sends general query messages to solicit group membership information. Hosts on the network that are members of a multicast group send report messages. When a host leaves a group, it sends a leave group message.

IGMP version 3 (IGMPv3) supports inclusion and exclusion lists. Inclusion lists enable you to specify which sources can send to a multicast group. This type of multicast group is called a source-specific multicast (SSM) group, and its multicast address is 232/8.

IGMPv3 provides support for source filtering. For example, a router can specify particular routers from which it accepts or rejects traffic. With IGMPv3, a multicast router can learn which sources are of interest to neighboring routers.

Exclusion mode works the opposite of an inclusion list. It allows any source but the ones listed to send to the SSM group.

IGMPv3 interoperates with versions 1 and 2 of the protocol. However, to remain compatible with older IGMP hosts and routers, IGMPv3 routers must also implement versions 1 and 2 of the protocol. IGMPv3 supports the following membership-report record types: mode is allowed, allow new sources, and block old sources.

Configuring IGMP

Before you begin:

1. Determine whether the router is directly attached to any multicast sources. Receivers must be able to locate these sources.
2. Determine whether the router is directly attached to any multicast group receivers. If receivers are present, IGMP is needed.
3. Determine whether to configure multicast to use sparse, dense, or sparse-dense mode. Each mode has different configuration considerations.
4. Determine the address of the RP if sparse or sparse-dense mode is used.
5. Determine whether to locate the RP with the static configuration, BSR, or auto-RP method.
6. Determine whether to configure multicast to use its own RPF routing table when configuring PIM in sparse, dense, or sparse-dense mode.
7. Configure the SAP and SDP protocols to listen for multicast session announcements. See *Configuring the Session Announcement Protocol*.

To configure the Internet Group Management Protocol (IGMP), include the **igmp** statement:

```
igmp {
  accounting;
  interface interface-name {
    disable;
    (accounting | no-accounting);
    group-policy [ policy-names ];
    immediate-leave;
    oif-map map-name;
    promiscuous-mode;
    ssm-map ssm-map-name;
    static {
      group multicast-group-address {
        exclude;
        group-count number;
        group-increment increment;
        source ip-address {
          source-count number;
          source-increment increment;
        }
      }
    }
  }
  version version;
}
query-interval seconds;
query-last-member-interval seconds;
query-response-interval seconds;
robust-count number;
traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable>;
```

```
    flag flag <flag-modifier> <disable>;  
  }  
}
```

You can include this statement at the following hierarchy levels:

- [edit protocols]
- [edit logical-systems *logical-system-name* protocols]

By default, IGMP is enabled on all interfaces on which you configure Protocol Independent Multicast (PIM), and on all broadcast interfaces on which you configure the Distance Vector Multicast Routing Protocol (DVMRP).



NOTE: You can configure IGMP on an interface without configuring PIM. PIM is generally not needed on IGMP downstream interfaces. Therefore, only one “pseudo PIM interface” is created to represent all IGMP downstream (IGMP-only) interfaces on the router. This reduces the amount of router resources, such as memory, that are consumed. You must configure PIM on upstream IGMP interfaces to enable multicast routing, perform reverse-path forwarding for multicast data packets, populate the multicast forwarding table for upstream interfaces, and in the case of bidirectional PIM and PIM sparse mode, to distribute IGMP group memberships into the multicast routing domain.

Enabling IGMP

The Internet Group Management Protocol (IGMP) manages multicast groups by establishing, maintaining, and removing groups on a subnet. Multicast routing devices use IGMP to learn which groups have members on each of their attached physical networks. IGMP must be enabled for the router to receive IPv4 multicast packets. IGMP is only needed for IPv4 networks, because multicast is handled differently in IPv6 networks. IGMP is automatically enabled on all IPv4 interfaces on which you configure PIM and on all IPv4 broadcast interfaces when you configure DVMRP.

If IGMP is not running on an interface—either because PIM and DVMRP are not configured on the interface or because IGMP is explicitly disabled on the interface—you can explicitly enable IGMP.

To explicitly enable IGMP:

1. If PIM and DVMRP are not running on the interface, explicitly enable IGMP by including the interface name.

```
[edit protocols igmp]  
user@host# set interface fe-0/0/0.0
```

2. See if IGMP is disabled on any interfaces. In the following example, IGMP is disabled on a Gigabit Ethernet interface.

```
[edit protocols igmp]  
user@host# show
```

```
interface fe-0/0/0.0;
interface ge-1/0/0.0 {
  disable;
}
```

3. Enable IGMP on the interface by deleting the **disable** statement.

```
[edit protocols igmp]
delete interface ge-1/0/0.0 disable
```

4. Verify the configuration.

```
[edit protocols igmp]
user@host# show
interface fe-0/0/0.0;
interface ge-1/0/0.0;
```

5. Verify the operation of IGMP on the interfaces by checking the output of the **show igmp interface** command.

Modifying the IGMP Host-Query Message Interval

The objective of IGMP is to keep routers up to date with group membership of the entire subnet. Routers need not know who all the members are, only that members exist. Each host keeps track of which multicast groups are subscribed to. On each link, one router is elected the querier. The IGMP querier router periodically sends general host-query messages on each attached network to solicit membership information. The messages are sent to the all-systems multicast group address, 224.0.0.1.

The query interval, the response interval, and the robustness variable are related in that they are all variables that are used to calculate the group membership timeout. The group membership timeout is the number of seconds that must pass before a multicast router determines that no more members of a host group exist on a subnet. The group membership timeout is calculated as the (robustness variable x query-interval) + (query-response-interval). If no reports are received for a particular group before the group membership timeout has expired, the routing device stops forwarding remotely-originated multicast packets for that group onto the attached network.

By default, host-query messages are sent every 125 seconds. You can change this interval to change the number of IGMP messages sent on the subnet.

To modify the query interval:

1. Configure the interval.

```
[edit protocols igmp]
user@host# set query-interval 200
```

The value can be from 1 through 1024 seconds.

2. Verify the configuration by checking the IGMP Query Interval field in the output of the **show igmp interface** command.
3. Verify the operation of the query interval by checking the Membership Query field in the output of the **show igmp statistics** command.

Modifying the IGMP Query Response Interval

The query response interval is the maximum amount of time that can elapse between when the querier router sends a host-query message and when it receives a response from a host. Configuring this interval allows you to adjust the burst peaks of IGMP messages on the subnet. Set a larger interval to make the traffic less bursty. Bursty traffic refers to an uneven pattern of data transmission: sometimes a very high data transmission rate, whereas at other times a very low data transmission rate.

The query response interval, the host-query interval, and the robustness variable are related in that they are all variables that are used to calculate the group membership timeout. The group membership timeout is the number of seconds that must pass before a multicast router determines that no more members of a host group exist on a subnet. The group membership timeout is calculated as the (robustness variable x query-interval) + (query-response-interval). If no reports are received for a particular group before the group membership timeout has expired, the routing device stops forwarding remotely originated multicast packets for that group onto the attached network.

The default query response interval is 10 seconds. You can configure a subsecond interval up to one digit to the right of the decimal point. The configurable range is 0.1 through 0.9, then in 1-second intervals 1 through 999,999.

To modify the query response interval:

1. Configure the interval.

```
[edit protocols igmp]  
user@host# set query-response-interval 0.4
```

2. Verify the configuration by checking the IGMP Query Response Interval field in the output of the **show igmp interface** command.
3. Verify the operation of the query interval by checking the Membership Query field in the output of the **show igmp statistics** command.

Specifying Immediate-Leave Host Removal for IGMP

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.

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.

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.

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.



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.

To enable immediate leave on an interface:

1. Configure immediate leave on the IGMP interface.

```
[edit protocols IGMP]
user@host# set interface ge-0/0/0.1 immediate-leave
```

2. Verify the configuration by checking the Immediate Leave field in the output of the `show igmp interface` command.

Filtering Unwanted IGMP Reports at the IGMP Interface Level

Suppose you need to limit the subnets that can join a certain multicast group. The **group-policy** statement enables you to filter unwanted IGMP reports at the interface level. When this statement is enabled on a router running IGMP version 2 (IGMPv2) or version 3 (IGMPv3), after the router receives an IGMP report, the router compares the group against the specified group policy and performs the action configured in that policy (for example, rejects the report if the policy matches the defined address or network).

You define the policy to match only IGMP group addresses (for IGMPv2) by using the policy's **route-filter** statement to match the group address. You define the policy to match IGMP (source, group) addresses (for IGMPv3) by using the policy's **route-filter** statement to match the group address and the policy's **source-address-filter** statement to match the source address.



CAUTION: On MX Series platforms, IGMPv2 and IGMPv3 cannot be configured together on the same interface. Configuring both together causes unexpected behavior in multicast traffic forwarding.

To filter unwanted IGMP reports:

1. Configure an IGMPv2 policy.

```
[edit policy-statement reject_policy_v2]
```

```

user@host# set from route-filter 224.1.1.1/32 exact
user@host# set from route-filter 239.0.0.0/8 orlonger
user@host# set then reject

```

2. Configure an IGMPv3 policy.

```

[edit policy-statement reject_policy_v3]
user@host# set from route-filter 224.1.1.1/32 exact
user@host# set from route-filter 239.0.0.0/8 orlonger
user@host# set from source-address-filter 10.0.0.0/8 orlonger
user@host# set from source-address-filter 127.0.0.0/8 orlonger
user@host# set then reject

```

3. Apply the policies to the IGMP interfaces on which you prefer not to receive specific group or (source, group) reports. In this example, **ge-0/0/0.1** is running IGMPv2, and **ge-0/1/1.0** is running IGMPv3.

```

[edit protocols igmp]
user@host# set interface ge-0/0/0.1 group-policy reject_policy_v2
user@host# set interface ge-0/1/1.0 group-policy reject_policy_v3

```

4. Verify the operation of the filter by checking the Rejected Report field in the output of the **show igmp statistics** command.

Accepting IGMP Messages from Remote Subnetworks

By default, IGMP interfaces accept IGMP messages only from the same subnet. Including the **promiscuous-mode** statement enables the routing device to accept IGMP messages from indirectly connected subnets.



NOTE: When you enable IGMP on an unnumbered Ethernet interface that uses a /32 loopback address as a donor address, you must configure IGMP promiscuous mode to accept the IGMP packets received on this interface.



NOTE: When enabling promiscuous-mode, all routers on the ethernet segment must be configured with the promiscuous mode statement. Otherwise, only the interface configured with lowest IPv4 address acts as the querier for IGMP for this Ethernet segment.

To enable IGMP promiscuous mode on an interface:

1. Configure the IGMP interface.

```

[edit protocols igmp]
user@host# set interface ge-0/1/1.0 promiscuous-mode

```

2. Verify the configuration by checking the Promiscuous Mode field in the output of the **show igmp interface** command.
3. Verify the operation of the filter by checking the Rx non-local field in the output of the **show igmp statistics** command.

Modifying the IGMP Last-Member Query Interval

The last-member query interval is the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You can configure this interval to change the amount of time it takes a routing device to detect the loss of the last member of a group.

When the routing device that is serving as the querier receives a leave-group message from a host, the routing device sends multiple group-specific queries to the group being left. The querier sends a specific number of these queries at a specific interval. The number of queries sent is called the last-member query count. The interval at which the queries are sent is called the last-member query interval. Because both settings are configurable, you can adjust the leave latency. The IGMP leave latency is the time between a request to leave a multicast group and the receipt of the last byte of data for the multicast group.

The last-member query count x (times) the last-member query interval = (equals) the amount of time it takes a routing device to determine that the last member of a group has left the group and to stop forwarding group traffic.

The default last-member query interval is 1 second. You can configure a subsecond interval up to one digit to the right of the decimal point. The configurable range is 0.1 through 0.9, then in 1-second intervals 1 through 999,999.

To modify this interval:

1. Configure the time (in seconds) that the routing device waits for a report in response to a group-specific query.

```
[edit protocols igmp]
```

```
user@host# set query-last-member-interval 0.1
```

2. Verify the configuration by checking the IGMP Last Member Query Interval field in the output of the **show igmp interfaces** command.



NOTE: You can configure the last-member query count by configuring the robustness variable. The two are always equal.

Modifying the IGMP Robustness Variable

Fine-tune the IGMP robustness variable to allow for expected packet loss on a subnet. The robust count automatically changes certain IGMP message intervals for IGMPv2 and IGMPv3. Increasing the robust count allows for more packet loss but increases the leave latency of the subnetwork.

When the query router receives an IGMP leave message on a shared network running IGMPv2, the query router must send an IGMP group query message a specified number of times. The number of IGMP group query messages sent is determined by the robust count.

The value of the robustness variable is also used in calculating the following IGMP message intervals:

- Group member interval—Amount of time that must pass before a multicast router determines that there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query-interval) + (1 x query-response-interval).
- Other querier present interval—The robust count is used to calculate the amount of time that must pass before a multicast router determines that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query-interval) + (0.5 x query-response-interval).
- Last-member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The number of queries is equal to the value of the robustness variable.

In IGMPv3, a change of interface state causes the system to immediately transmit a state-change report from that interface. In case the state-change report is missed by one or more multicast routers, it is retransmitted. The number of times it is retransmitted is the robust count minus one. In IGMPv3, the robust count is also a factor in determining the group membership interval, the older version querier interval, and the other querier present interval.

By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to lose packets.

The number can be from 2 through 10.

To change the value of the robustness variable:

1. Configure the robust count.

When you set the robust count, you are in effect configuring the number of times the querier retries queries on the connected subnets.

```
[edit protocols igmp]  
user@host# set robust-count 5
```

2. Verify the configuration by checking the IGMP Robustness Count field in the output of the **show igmp interfaces** command.

Limiting the Maximum IGMP Message Rate

This section describes how to change the limit for the maximum number of IGMP packets transmitted in 1 second by the router.

Increasing the maximum number of IGMP packets transmitted per second might be useful on a router with a large number of interfaces participating in IGMP.

To change the limit for the maximum number of IGMP packets the router can transmit in 1 second, include the **maximum-transmit-rate** statement and specify the maximum number of packets per second to be transmitted.

Changing the IGMP Version

By default, the routing device runs IGMPv2. Routing devices running different versions of IGMP determine the lowest common version of IGMP that is supported by hosts on their subnet and operate in that version.

To enable source-specific multicast (SSM) functionality, you must configure version 3 on the host and the host's directly connected routing device. If a source address is specified in a multicast group that is statically configured, the version must be set to IGMPv3.

If a static multicast group is configured with the source address defined, and the IGMP version is configured to be version 2, the source is ignored and only the group is added. In this case, the join is treated as an IGMPv2 group join.

If you configure the IGMP version setting at the individual interface hierarchy level, it overrides the **interface all** statement.

If you have already configured the routing device to use IGMP version 1 (IGMPv1) and then configure it to use IGMPv2, the routing device continues to use IGMPv1 for up to 6 minutes and then uses IGMPv2.

To change to IGMPv3 for SSM functionality:

1. Configure the IGMP interface.

```
[edit protocols igmp]
user@host# set interface ge-0/0/0 version 3
```

2. Verify the configuration by checking the version field in the output of the **show igmp interfaces** command. The **show igmp statistics** command has version-specific output fields, such as V1 Membership Report, V2 Membership Report, and V3 Membership Report.



CAUTION: On MX Series platforms, IGMPv2 and IGMPv3 cannot be configured together on the same interface. Configuring both together causes unexpected behavior in multicast traffic forwarding.

Enabling IGMP Static Group Membership

You can create IGMP static group membership to test multicast forwarding without a receiver host. When you enable IGMP static group membership, data is forwarded to an interface without that interface receiving membership reports from downstream hosts. The router on which you enable static IGMP group membership must be the designated router (DR) for the subnet. Otherwise, traffic does not flow downstream.

When enabling IGMP static group membership, you cannot configure multiple groups using the **group-count**, **group-increment**, **source-count**, and **source-increment** statements if the **all** option is specified as the IGMP interface.

Class-of-service (CoS) adjustment is not supported with IGMP static group membership.

In this example, you create static group 225.1.1.1.

1. On the DR, configure the static groups to be created by including the **static** statement and **group** statement and specifying which IP multicast address of the group to be created. When creating groups individually, you must specify a unique address for each group.

```
[edit protocols igmp]
user@host# set interface fe-0/1/2 static group 225.1.1.1
```

2. After you commit the configuration, use the **show configuration protocol igmp** command to verify the IGMP protocol configuration.

```
user@host> show configuration protocol igmp

interface fe-0/1/2.0 {
  static {
    group 225.1.1.1 ;
  }
}
```

3. After you have committed the configuration and the source is sending traffic, use the **show igmp group** command to verify that static group 225.1.1.1 has been created.

```
user@host> show igmp group
Interface: fe-0/1/2
Group: 225.1.1.1
Source: 10.0.0.2
Last reported by: Local
Timeout: 0 Type: Static
```



NOTE: When you configure static IGMP group entries on point-to-point links that connect routing devices to a rendezvous point (RP), the static IGMP group entries do not generate join messages toward the RP.

When you create IGMP static group membership to test multicast forwarding on an interface on which you want to receive multicast traffic, you can specify that a number of static groups be automatically created. This is useful when you want to test forwarding to multiple receivers without having to configure each receiver separately.

In this example, you create three groups.

1. On the DR, configure the number of static groups to be created by including the **group-count** statement and specifying the number of groups to be created.

```
[edit protocols igmp]
user@host# set interface fe-0/1/2 static group 225.1.1.1 group-count 3
```

2. After you commit the configuration, use the **show configuration protocol igmp** command to verify the IGMP protocol configuration.

```
user@host> show configuration protocol igmp

interface fe-0/1/2.0 {
  static {
    group 225.1.1.1 {
      group-count 3;
    }
  }
}
```

3. After you have committed the configuration and after the source is sending traffic, use the **show igmp group** command to verify that static groups 225.1.1.1, 225.1.1.2, and 225.1.1.3 have been created.

```
user@host> show igmp group
Interface: fe-0/1/2
  Group: 225.1.1.1
    Source: 10.0.0.2
    Last reported by: Local
    Timeout: 0 Type: Static
  Group: 225.1.1.2
    Source: 10.0.0.2
    Last reported by: Local
    Timeout: 0 Type: Static
  Group: 225.1.1.3
    Source: 10.0.0.2
    Last reported by: Local
    Timeout: 0 Type: Static
```

When you create IGMP static group membership to test multicast forwarding on an interface on which you want to receive multicast traffic, you can also configure the group address to be automatically incremented for each group created. This is useful when you want to test forwarding to multiple receivers without having to configure each receiver separately and when you do not want the group addresses to be sequential.

In this example, you create three groups and increase the group address by an increment of two for each group.

1. On the DR, configure the group address increment by including the **group-increment** statement and specifying the number by which the address should be incremented for each group. The increment is specified in dotted decimal notation similar to an IPv4 address.

```
[edit protocols igmp]
user@host# set interface fe-0/1/2 static group 225.1.1.1 group-count 3 group-increment
0.0.0.2
```

2. After you commit the configuration, use the **show configuration protocol igmp** command to verify the IGMP protocol configuration.

```
user@host> show configuration protocol igmp

interface fe-0/1/2.0 {
  version 3;
  static {
```

```
group 225.1.1.1 {  
    group-increment 0.0.0.2;  
    group-count 3;  
}  
}
```

3. After you have committed the configuration and after the source is sending traffic, use the **show igmp group** command to verify that static groups 225.1.1.1, 225.1.1.3, and 225.1.1.5 have been created.

```
user@host> show igmp group  
Interface: fe-0/1/2  
  Group: 225.1.1.1  
    Source: 10.0.0.2  
    Last reported by: Local  
    Timeout: 0 Type: Static  
  Group: 225.1.1.3  
    Source: 10.0.0.2  
    Last reported by: Local  
    Timeout: 0 Type: Static  
  Group: 225.1.1.5  
    Source: 10.0.0.2  
    Last reported by: Local  
    Timeout: 0 Type: Static
```

When you create IGMP static group membership to test multicast forwarding on an interface on which you want to receive multicast traffic, and your network is operating in source-specific multicast (SSM) mode, you can also specify that the multicast source address be accepted. This is useful when you want to test forwarding to multicast receivers from a specific multicast source.

If you specify a group address in the SSM range, you must also specify a source.

If a source address is specified in a multicast group that is statically configured, the IGMP version on the interface must be set to IGMPv3. IGMPv2 is the default value.

In this example, you create group 225.1.1.1 and accept IP address 10.0.0.2 as the only source.

1. On the DR, configure the source address by including the **source** statement and specifying the IPv4 address of the source host.

```
[edit protocols igmp]  
user@host# set interface fe-0/1/2 static group 225.1.1.1 source 10.0.0.2
```

2. After you commit the configuration, use the **show configuration protocol igmp** command to verify the IGMP protocol configuration.

```
user@host> show configuration protocol igmp  
interface fe-0/1/2.0 {  
    version 3;  
    static {  
        group 225.1.1.1 {  
            source 10.0.0.2;  
        }  
    }  
}
```

```
}
```

3. After you have committed the configuration and the source is sending traffic, use the **show igmp group** command to verify that static group 225.1.1.1 has been created and that source 10.0.0.2 has been accepted.

```
user@host> show igmp group
Interface: fe-0/1/2
  Group: 225.1.1.1
    Source: 10.0.0.2
    Last reported by: Local
    Timeout: 0 Type: Static
```

When you create IGMP static group membership to test multicast forwarding on an interface on which you want to receive multicast traffic, you can specify that a number of multicast sources be automatically accepted. This is useful when you want to test forwarding to multicast receivers from more than one specified multicast source.

In this example, you create group 255.1.1.1 and accept addresses 10.0.0.2, 10.0.0.3, and 10.0.0.4 as the sources.

1. On the DR, configure the number of multicast source addresses to be accepted by including the **source-count** statement and specifying the number of sources to be accepted.

```
[edit protocols igmp]
user@host# set interface fe-0/1/2 static group 225.1.1.1 source 10.0.0.2 source-count
3
```

2. After you commit the configuration, use the **show configuration protocol igmp** command to verify the IGMP protocol configuration.

```
user@host> show configuration protocol igmp

interface fe-0/1/2.0 {
  version 3;
  static {
    group 225.1.1.1 {
      source 10.0.0.2 {
        source-count 3;
      }
    }
  }
}
```

3. After you have committed the configuration and the source is sending traffic, use the **show igmp group** command to verify that static group 225.1.1.1 has been created and that sources 10.0.0.2, 10.0.0.3, and 10.0.0.4 have been accepted.

```
user@host> show igmp group
Interface: fe-0/1/2
  Group: 225.1.1.1
    Source: 10.0.0.2
    Last reported by: Local
    Timeout: 0 Type: Static
  Group: 225.1.1.1
    Source: 10.0.0.3
    Last reported by: Local
    Timeout: 0 Type: Static
```

```
Group: 225.1.1.1
Source: 10.0.0.4
Last reported by: Local
Timeout: 0 Type: Static
```

When you configure static groups on an interface on which you want to receive multicast traffic, and specify that a number of multicast sources be automatically accepted, you can also specify the number by which the address should be incremented for each source accepted. This is useful when you want to test forwarding to multiple receivers without having to configure each receiver separately and you do not want the source addresses to be sequential.

In this example, you create group 225.1.1.1 and accept addresses 10.0.0.2, 10.0.0.4, and 10.0.0.6 as the sources.

1. Configure the multicast source address increment by including the **source-increment** statement and specifying the number by which the address should be incremented for each source. The increment is specified in dotted decimal notation similar to an IPv4 address.

```
[edit protocols igmp]
```

```
user@host# set interface fe-0/1/2 static group 225.1.1.1 source 10.0.0.2 source-count 3 source-increment 0.0.0.2
```

2. After you commit the configuration, use the **show configuration protocol igmp** command to verify the IGMP protocol configuration.

```
user@host> show configuration protocol igmp
```

```
interface fe-0/1/2.0 {
  version 3;
  static {
    group 225.1.1.1 {
      source 10.0.0.2 {
        source-count 3;
        source-increment 0.0.0.2;
      }
    }
  }
}
```

3. After you have committed the configuration and after the source is sending traffic, use the **show igmp group** command to verify that static group 225.1.1.1 has been created and that sources 10.0.0.2, 10.0.0.4, and 10.0.0.6 have been accepted.

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

```
Interface: fe-0/1/2
  Group: 225.1.1.1
    Source: 10.0.0.2
    Last reported by: Local
    Timeout: 0 Type: Static
  Group: 225.1.1.1
    Source: 10.0.0.4
    Last reported by: Local
    Timeout: 0 Type: Static
  Group: 225.1.1.1
    Source: 10.0.0.6
```

Last reported by: Local
Timeout: 0 Type: Static

When you configure static groups on an interface on which you want to receive multicast traffic and your network is operating in source-specific multicast (SSM) mode, you can specify that certain multicast source addresses be excluded.

By default the multicast source address configured in a static group operates in include mode. In include mode the multicast traffic for the group is accepted from the source address configured. You can also configure the static group to operate in exclude mode. In exclude mode the multicast traffic for the group is accepted from any address other than the source address configured.

If a source address is specified in a multicast group that is statically configured, the IGMP version on the interface must be set to IGMPv3. IGMPv2 is the default value.

In this example, you exclude address 10.0.0.2 as a source for group 225.1.1.1.

1. On the DR, configure a multicast static group to operate in exclude mode by including the **exclude** statement and specifying which IPv4 source address to exclude.

```
[edit protocols igmp]
user@host# set interface fe-0/1/2 static group 225.1.1.1 exclude source 10.0.0.2
```

2. After you commit the configuration, use the **show configuration protocol igmp** command to verify the IGMP protocol configuration.

```
user@host> show configuration protocol igmp

interface fe-0/1/2.0 {
  version 3;
  static {
    group 225.1.1.1 {
      exclude;
      source 10.0.0.2;
    }
  }
}
```

3. After you have committed the configuration and the source is sending traffic, use the **show igmp group detail** command to verify that static group 225.1.1.1 has been created and that the static group is operating in exclude mode.

```
user@host> show igmp group detail
Interface: fe-0/1/2
Group: 225.1.1.1
Group mode: Exclude
Source: 10.0.0.2
Last reported by: Local
Timeout: 0 Type: Static
```

Recording IGMP Join and Leave Events

To determine whether IGMP tuning is needed in a network, you can configure the routing device to record IGMP join and leave events. You can record events globally for the routing device or for individual interfaces.

Table 4 on page 38 describes the recordable IGMP events.

Table 4: IGMP Event Messages

ERRMSG Tag	Definition
RPD_IGMP_JOIN	Records IGMP join events.
RPD_IGMP_LEAVE	Records IGMP leave events.
RPD_IGMP_ACCOUNTING_ON	Records when IGMP accounting is enabled on an IGMP interface.
RPD_IGMP_ACCOUNTING_OFF	Records when IGMP accounting is disabled on an IGMP interface.
RPD_IGMP_MEMBERSHIP_TIMEOUT	Records IGMP membership timeout events.

To enable IGMP accounting:

1. Enable accounting globally or on an IGMP interface. This example shows both options.

```
[edit protocols igmp]
user@host# set accounting
user@host# set interface fe-0/1/0.2 accounting
```

2. Configure the events to be recorded and filter the events to a system log file with a descriptive filename, such as **igmp-events**.

```
[edit system syslog file igmp-events]
user@host# set any info
user@host# set match ".*RPD_IGMP_JOIN.* | .*RPD_IGMP_LEAVE.* |
.*RPD_IGMP_ACCOUNTING.* | .*RPD_IGMP_MEMBERSHIP_TIMEOUT.*"
```

3. Periodically archive the log file.

This example rotates the file size when it reaches 100 KB and keeps three files.

```
[edit system syslog file igmp-events]
user@host# set archive size 100000
user@host# set archive files 3
user@host# set archive archive-sites "ftp://user@host1//var/tmp" password
"anonymous"
user@host# set archive archive-sites "ftp://user@host2//var/tmp" password "test"
user@host# set archive transfer-interval 24
user@host# set archive start-time 2011-01-07:12:30
```

4. You can monitor the system log file as entries are added to the file by running the **monitor start** and **monitor stop** commands.

```
user@host> monitor start igmp-events

*** igmp-events ***
Apr 16 13:08:23 host mgd[16416]: UI_CMDLINE_READ_LINE: User 'user', command
'run monitor start igmp-events '
monitor
```


Limiting the Number of IGMP Multicast Group Joins on Logical Interfaces

The **group-limit** statement enables you to limit the number of IGMP multicast group joins for logical interfaces. When this statement is enabled on a router running IGMP version 2 (IGMPv2) or version 3 (IGMPv3), the limit is applied upon receipt of the group report. Once the group limit is reached, subsequent join requests are rejected.

When configuring limits for IGMP multicast groups, keep the following in mind:

- Each any-source group (*G) counts as one group toward the limit.
- Each source-specific group (S,G) counts as one group toward the limit.
- Groups in IGMPv3 exclude mode are counted toward the limit.
- Multiple source-specific groups count individually toward the group limit, even if they are for the same group. For example, (S1, G1) and (S2, G1) would count as two groups toward the configured limit.
- Combinations of any-source groups and source-specific groups count individually toward the group limit, even if they are for the same group. For example, (*, G1) and (S, G1) would count as two groups toward the configured limit.
- Configuring and committing a group limit on a network that is lower than what already exists on the network results in the removal of all groups from the configuration. The groups must then request to rejoin the network (up to the newly configured group limit).
- You can dynamically limit multicast groups on IGMP logical interfaces using dynamic profiles.

Beginning with Junos OS 12.2, you can optionally configure a system log warning threshold for IGMP multicast group joins received on the logical interface. It is helpful to review the system log messages for troubleshooting purposes and to detect if an excessive amount of IGMP multicast group joins have been received on the interface. These log messages convey when the configured group limit has been exceeded, when the configured threshold has been exceeded, and when the number of groups drop below the configured threshold.

The **group-threshold** statement enables you to configure the threshold at which a warning message is logged. The range is 1 through 100 percent. The warning threshold is a percentage of the group limit, so you must configure the **group-limit** statement to configure a warning threshold. For instance, when the number of groups exceed the configured warning threshold, but remain below the configured group limit, multicast groups continue to be accepted, and the device logs the warning message. In addition, the device logs a warning message after the number of groups drop below the configured warning threshold. You can further specify the amount of time (in seconds) between the log messages by configuring the **log-interval** statement. The range is 6 through 32,767 seconds.

You might consider throttling log messages because every entry added after the configured threshold and every entry rejected after the configured limit causes a warning message to be logged. By configuring a log interval, you can throttle the amount of system log warning messages generated for IGMP multicast group joins.

To limit multicast group joins on an IGMP logical interface:

1. Access the logical interface at the IGMP protocol hierarchy level.

```
[edit]
user@host# edit protocols igmp interface interface-name
```

2. Specify the group limit for the interface.

```
[edit protocols igmp interface interface-name]
user@host# set group-limit limit
```

3. (Optional) Configure the threshold at which a warning message is logged.

```
[edit protocols igmp interface interface-name]
user@host# set group-threshold value
```

4. (Optional) Configure the amount of time between log messages.

```
[edit protocols igmp interface interface-name]
user@host# set log-interval seconds
```

To confirm your configuration, use the **show protocols igmp** command. To verify the operation of IGMP on the interface, including the configured group limit and the optional warning threshold and interval between log messages, use the **show igmp interface** command.

Tracing IGMP Protocol Traffic

Tracing operations record detailed messages about the operation of routing protocols, such as the various types of routing protocol packets sent and received, and routing policy actions. You can specify which trace operations are logged by including specific tracing flags. The following table describes the flags that you can include.

Flag	Description
all	Trace all operations.
client-notification	Trace notifications.
general	Trace general flow.
group	Trace group operations.
host-notification	Trace host notifications.
leave	Trace leave group messages (IGMPv2 only).
mtrace	Trace mtrace packets. Use the mtrace command to troubleshoot the software.
normal	Trace normal events.
packets	Trace all IGMP packets.

Flag	Description
policy	Trace policy processing.
query	Trace IGMP membership query messages, including general and group-specific queries.
report	Trace membership report messages.
route	Trace routing information.
state	Trace state transitions.
task	Trace task processing.
timer	Trace timer processing.

In the following example, tracing is enabled for all routing protocol packets. Then tracing is narrowed to focus only on IGMP packets of a particular type. To configure tracing operations for IGMP:

1. (Optional) Configure tracing at the routing options level to trace all protocol packets.

```
[edit routing-options traceoptions]
user@host# set file all-packets-trace
user@host# set flag all
```

2. Configure the filename for the IGMP trace file.

```
[edit protocols igmp traceoptions]
user@host# set file igmp-trace
```

3. (Optional) Configure the maximum number of trace files.

```
[edit protocols igmp traceoptions]
user@host# set file files 5
```

4. (Optional) Configure the maximum size of each trace file.

```
[edit protocols igmp traceoptions]
user@host# set file size 1m
```

5. (Optional) Enable unrestricted file access.

```
[edit protocols igmp traceoptions]
user@host# set file world-readable
```

6. Configure tracing flags. Suppose you are troubleshooting issues with a particular multicast group. The following example shows how to flag all events for packets associated with the group IP address.

```
[edit protocols igmp traceoptions]
user@host# set flag group | match 232.1.1.2
```

7. View the trace file.

```
user@host> file list /var/log
user@host> file show /var/log/igmp-trace
```

Disabling IGMP

To disable IGMP on an interface, include the **disable** statement:

```
disable;
```

You can include this statement at the following hierarchy levels:

- [edit protocols igmp interface *interface-name*]
- [edit logical-systems *logical-system-name* protocols igmp interface *interface-name*]

IGMP and Nonstop Active Routing

Nonstop active routing (NSR) configurations include two Routing Engines that share information so that routing is not interrupted during Routing Engine failover. These NSR configurations include passive support with IGMP in connection with PIM. The master Routing Engine uses IGMP to determine its PIM multicast state, and this IGMP-derived information is replicated on the backup Routing Engine. IGMP on the new master Routing Engine (after failover) relearns the state information quickly through IGMP operation. In the interim, the new master Routing Engine retains the IGMP-derived PIM state as received by the replication process from the old master Routing Engine. This state information times out unless refreshed by IGMP on the new master Routing Engine. No additional IGMP configuration is required.

Related Documentation

- *Examples: Configuring MLD*

CHAPTER 3

Managing Group Membership with MLD (IPv6)

- [Understanding MLD on page 43](#)
- [Understanding MLD Snooping on page 46](#)
- [Configuring MLD Snooping on a VLAN \(CLI Procedure\) on page 54](#)
- [Example: Configuring MLD Snooping on EX Series Switches on page 60](#)
- [Verifying MLD Snooping on page 63](#)
- [Configuring MLD Snooping Tracing Operations \(CLI Procedure\) on page 67](#)

Understanding MLD

The Multicast Listener Discovery (MLD) Protocol manages the membership of hosts and routers in multicast groups. IP version 6 (IPv6) multicast routers use MLD to learn, for each of their attached physical networks, which groups have interested listeners. Each routing device maintains a list of host multicast addresses that have listeners for each subnetwork, as well as a timer for each address. However, the routing device does not need to know the address of each listener—just the address of each host. The routing device provides addresses to the multicast routing protocol it uses, which ensures that multicast packets are delivered to all subnetworks where there are interested listeners. In this way, MLD is used as the transport for the Protocol Independent Multicast (PIM) Protocol.

MLD is an integral part of IPv6 and must be enabled on all IPv6 routing devices and hosts that need to receive IP multicast traffic. The Junos OS supports MLD versions 1 and 2. Version 2 is supported for source-specific multicast (SSM) include and exclude modes.

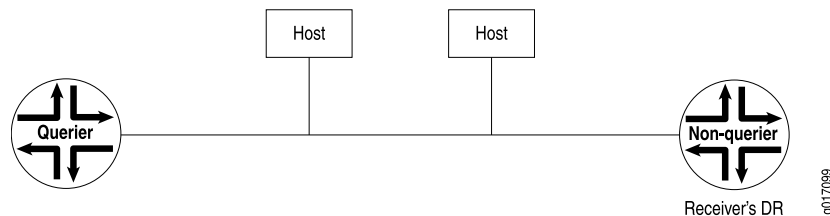
In include mode, the receiver specifies the source or sources it is interested in receiving the multicast group traffic from. Exclude mode works the opposite of include mode. It allows the receiver to specify the source or sources it is not interested in receiving the multicast group traffic from.

For each attached network, a multicast routing device can be either a querier or a nonquerier. A querier routing device, usually one per subnet, solicits group membership information by transmitting MLD queries. When a host reports to the querier routing device that it has interested listeners, the querier routing device forwards the membership information to the rendezvous point (RP) routing device by means of the receiver's

(host's) designated router (DR). This builds the rendezvous-point tree (RPT) connecting the host with interested listeners to the RP routing device. The RPT is the initial path used by the sender to transmit information to the interested listeners. Nonquerier routing devices do not transmit MLD queries on a subnet but can do so if the querier routing device fails.

All MLD-configured routing devices start as querier routing devices on each attached subnet (see [Figure 3 on page 44](#)). The querier routing device on the right is the receiver's DR.

Figure 3: Routing Devices Start Up on a Subnet

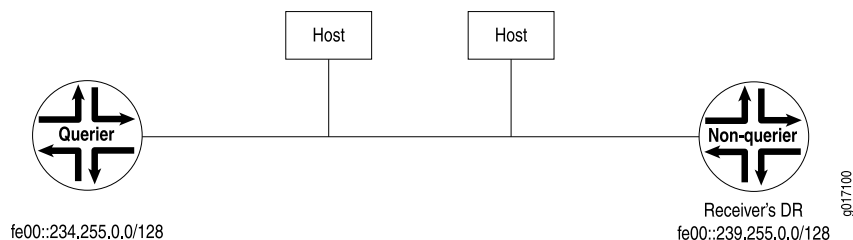


To elect the querier routing device, the routing devices exchange query messages containing their IPv6 source addresses. If a routing device hears a query message whose IPv6 source address is numerically lower than its own selected address, it becomes a nonquerier. In [Figure 4 on page 44](#), the routing device on the left has a source address numerically lower than the one on the right and therefore becomes the querier routing device.



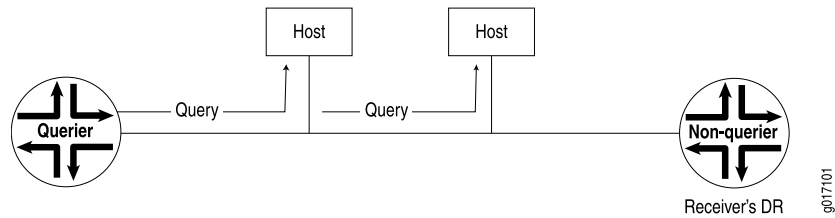
NOTE: In the practical application of MLD, several routing devices on a subnet are nonqueriers. If the elected querier routing device fails, query messages are exchanged among the remaining routing devices. The routing device with the lowest IPv6 source address becomes the new querier routing device. The IPv6 Neighbor Discovery Protocol (NDP) implementation drops incoming Neighbor Announcement (NA) messages that have a broadcast or multicast address in the target link-layer address option. This behavior is recommended by RFC 2461.

Figure 4: Querier Routing Device Is Determined



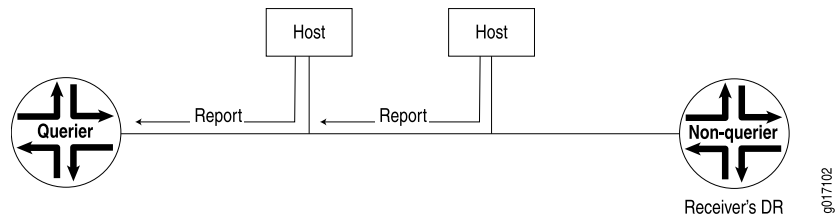
The querier routing device sends general MLD queries on the **link-scope all-nodes** multicast address FF02::1 at short intervals to all attached subnets to solicit group membership information (see [Figure 5 on page 45](#)). Within the query message is the *maximum response delay* value, specifying the maximum allowed delay for the host to respond with a report message.

Figure 5: General Query Message Is Issued



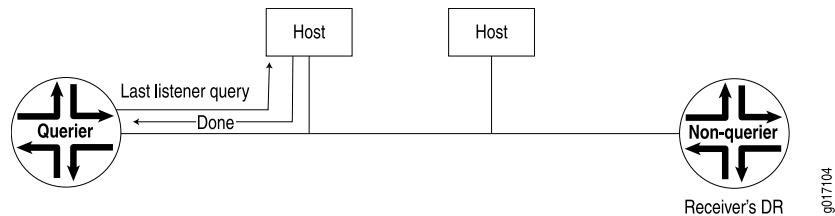
If interested listeners are attached to the host receiving the query, the host sends a report containing the host's IPv6 address to the routing device (see [Figure 6 on page 45](#)). If the reported address is not yet in the routing device's list of multicast addresses with interested listeners, the address is added to the list and a timer is set for the address. If the address is already on the list, the timer is reset. The host's address is transmitted to the RP in the PIM domain.

Figure 6: Reports Are Received by the Querier Routing Device



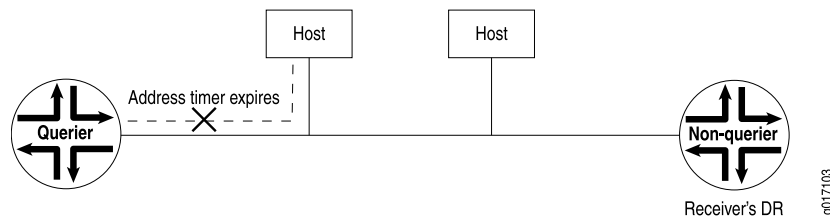
If the host has no interested multicast listeners, it sends a done message to the querier routing device. On receipt, the querier routing device issues a multicast address-specific query containing the last **listener query interval** value to the multicast address of the host. If the routing device does not receive a report from the multicast address, it removes the multicast address from the list and notifies the RP in the PIM domain of its removal (see [Figure 7 on page 45](#)).

Figure 7: Host Has No Interested Receivers and Sends a Done Message to Routing Device



If a done message is not received by the querier routing device, the querier routing device continues to send multicast address-specific queries. If the timer set for the address on receipt of the last report expires, the querier routing device assumes there are no longer interested listeners on that subnet, removes the multicast address from the list, and notifies the RP in the PIM domain of its removal (see [Figure 8 on page 46](#)).

Figure 8: Host Address Timer Expires and Address Is Removed from Multicast Address List



- Related Documentation**
- [Enabling MLD](#)
 - [Example: Recording MLD Join and Leave Events](#)
 - [Example: Modifying the MLD Robustness Variable](#)

Understanding MLD Snooping



NOTE: This overview 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 *Understanding MLD Snooping*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

Multicast Listener Discovery (MLD) snooping constrains the flooding of IPv6 multicast traffic on VLANs. When MLD snooping is enabled on a VLAN, a Juniper Networks EX Series Ethernet Switch examines MLD messages between hosts and multicast routers and learns which hosts are interested in receiving traffic for a multicast group. On the basis of 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.

MLD snooping supports MLD version 1 (MLDv1) and MLDv2. For details on MLDv1 and MLDv2, see the following standards:

- MLDv1—See RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*.
- MLDv2—See RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*.

This topic covers:

- [How MLD Snooping Works on page 47](#)
- [MLD Message Types on page 48](#)
- [How Hosts Join and Leave Multicast Groups on page 48](#)
- [Support for MLDv2 Multicast Sources on page 49](#)
- [MLD Snooping and Forwarding Interfaces on page 49](#)
- [General Forwarding Rules on page 50](#)
- [Examples of MLD Snooping Multicast Forwarding on page 50](#)

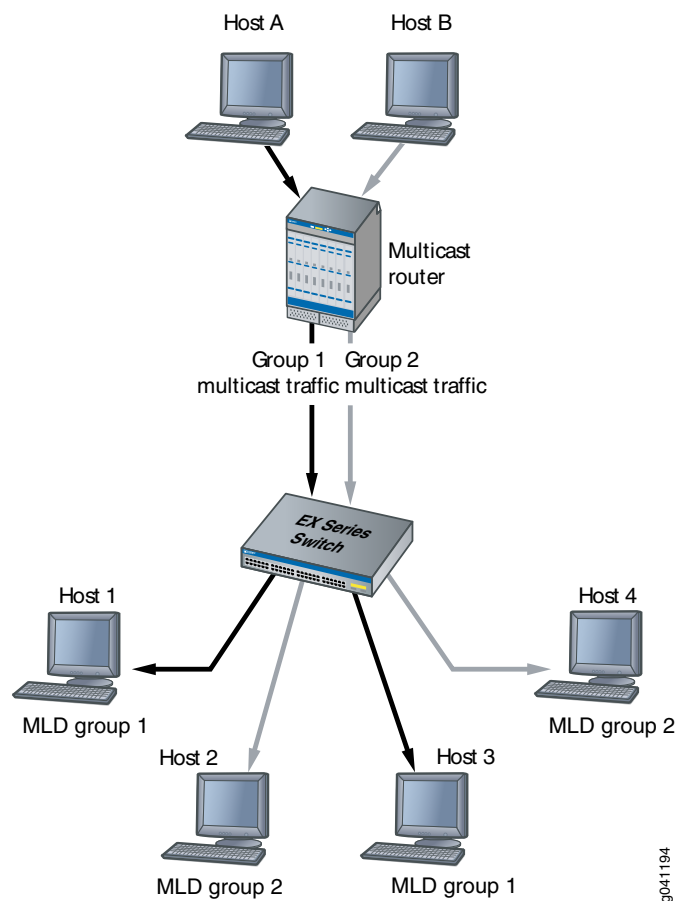
How MLD Snooping Works

By default, a switch floods Layer 2 multicast traffic on all of the interfaces belonging to that VLAN on a switch, except for the interface that is the source of the multicast traffic. This behavior can consume significant amounts of bandwidth.

You can enable MLD snooping to avoid this flooding. When you enable MLD snooping, the switch monitors MLD messages between receivers (hosts) and multicast routers and uses the content of the messages to build an IPv6 multicast forwarding table—a database of IPv6 multicast groups and the interfaces that are connected to the interested members of each group. 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 9 on page 47 shows an example of multicast traffic flow with MLD snooping enabled.

Figure 9: Multicast Traffic Flow with MLD Snooping Enabled



MLD Message Types

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

- General query—Asks whether any host is listening to any group.
- Group-specific query—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—(MLD version 2 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 no 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—Indicates that the host wants to leave a particular multicast group.

Strictly speaking, only MLDv1 hosts use two different kinds of reports to indicate whether they want to join or leave a group. MLDv2 hosts send only one kind of report, the contents of which indicate whether they want to join or leave a group. However, for simplicity's sake, the MLD snooping documentation uses the term *membership report* for a report that indicates that a host wants to join a group and uses the term *leave report* for a report that indicates a host wants to leave a group.

How Hosts Join and Leave Multicast Groups

Hosts can join multicast groups in either of two ways:

- By sending an unsolicited membership report that specifies the multicast group that the host is attempting to join.
- By sending a membership report in response to a query from a multicast router.

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

Hosts can leave multicast groups 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."
- By sending a leave report.



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 MLDv2 Multicast Sources

In MLDv2, 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.

MLD Snooping and Forwarding Interfaces

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

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

The switch learns about these interfaces by monitoring MLD traffic. If an interface receives MLD queries, 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 MLD queries 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 MLD querier must exist in the network. For the switch itself to function as an MLD querier, MLD 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 MLD snooping is enabled is forwarded according to the following rules.

MLD protocol traffic is forwarded as follows:

- MLD general queries received on a multicast-router interface are forwarded to all other interfaces in the VLAN.
- MLD group-specific queries received on a multicast-router interface are forwarded to only those interfaces in the VLAN that are members of the group.
- MLD 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 MLD protocol traffic is forwarded as follows:

- 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 MLD Snooping Multicast Forwarding

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

- [Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts on page 50](#)
- [Scenario 2: Switch Forwarding Multicast Traffic to Another Switch on page 51](#)
- [Scenario 3: Switch Connected to Hosts Only \(No MLD Querier\) on page 52](#)
- [Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs on page 53](#)

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

In the topology shown in [Figure 10 on page 51](#), a switch acting as a Layer 2 device receives multicast traffic belonging to multicast group **ff1e::2010** from Source A, which is connected to the multicast router. It also receives multicast traffic belonging to multicast group **ff15::2** from Source B, which is connected directly to the switch. All interfaces on the switch belong to the same VLAN.

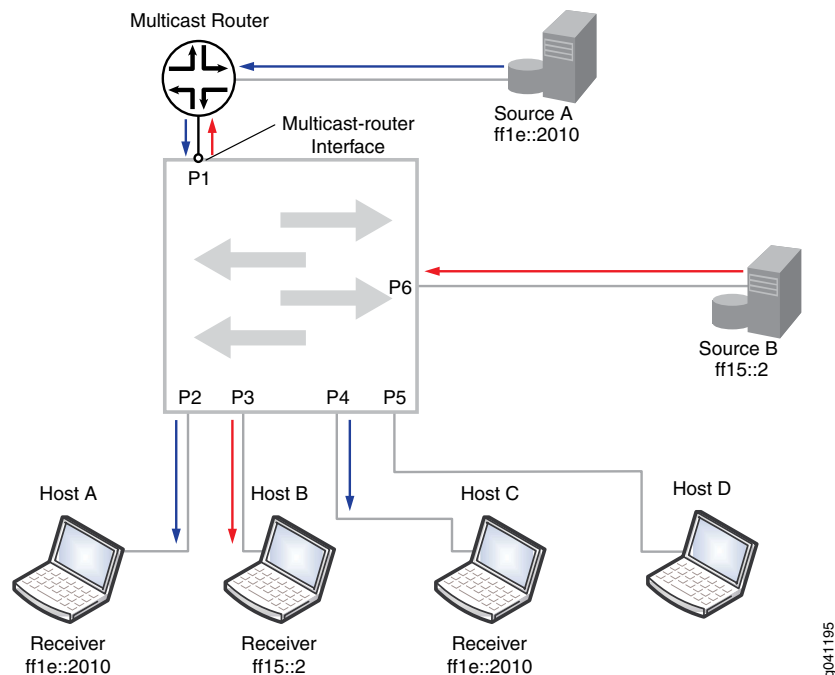
Because the switch receives MLD queries from the multicast router on interface P1, MLD snooping learns that interface P1 is a multicast-router interface and adds the interface to its multicast forwarding table. It forwards any MLD general queries it receives on this

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 general queries with membership reports for group **ff1e::2010**. MLD snooping adds interfaces P2 and P4 to its multicast forwarding table as member interfaces for group **ff1e::2010**. 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 general queries with a membership report for group **ff15::2**. The switch adds interface P3 to its multicast forwarding table as a member interface for group **ff15::2** 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 10: Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts



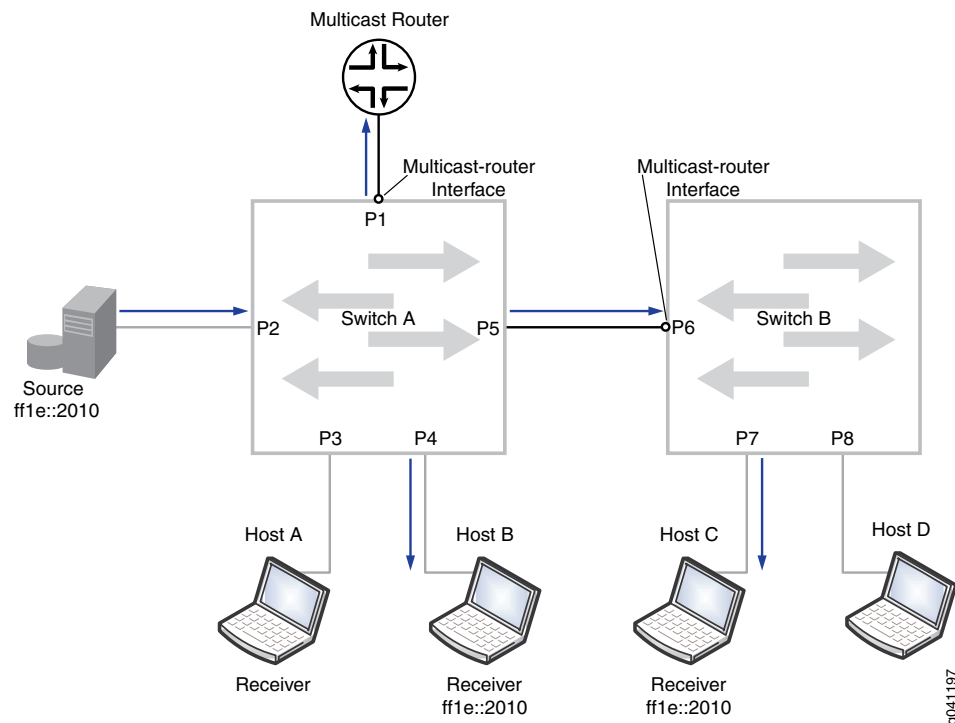
Scenario 2: Switch Forwarding Multicast Traffic to Another Switch

In the topology shown in [Figure 11 on page 52](#), 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 MLD queries from the multicast router on interface P1, making interface P1 a multicast-router interface for Switch A. Switch A forwards all general 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 MLD queries on interface P6, P6 is the multicast-router interface for Switch B. Switch B forwards the 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 forwarding table as a group-member interface, and forwards multicast traffic from the source to Switch B.

Figure 11: 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.

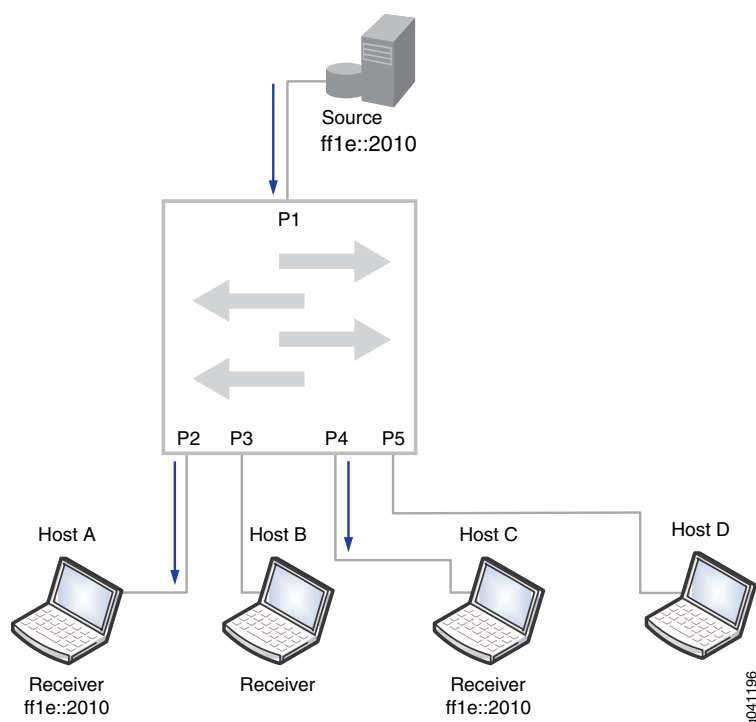
Scenario 3: Switch Connected to Hosts Only (No MLD Querier)

In the topology shown in Figure 12 on page 53, a switch is connected to a multicast source and to hosts. There is no multicast router in this topology—hence there is no MLD querier. Without an MLD querier to respond to, a host does not send periodic membership reports. As a result, even if the host sends an unsolicited membership report to join a multicast group, its membership in the multicast group will time out.

For MLD 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 MLD on it. In this case, the switch itself acts as an MLD querier, and the hosts can dynamically join the multicast group and refresh their group membership by responding to the queries.

Figure 12: Scenario 3: Switch Connected to Hosts Only (No MLD Querier)

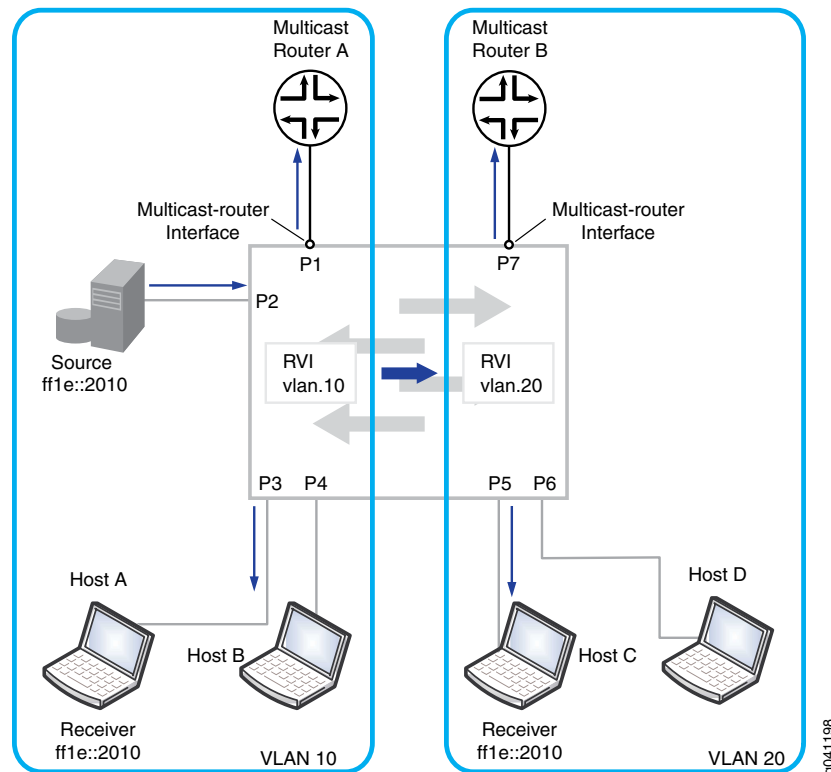


Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs

In the topology shown in [Figure 13 on page 54](#), 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.

Figure 13: Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs



- Related Documentation**
- *Example: Configuring MLD Snooping*
 - *Configuring MLD Snooping on a VLAN (CLI Procedure)*
 - *Verifying MLD Snooping (CLI Procedure)*

Configuring MLD Snooping on a VLAN (CLI Procedure)



NOTE: This task 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 MLD Snooping on a VLAN (CLI Procedure)*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

You can enable MLD snooping on a VLAN to constrain the flooding of IPv6 multicast traffic on the VLAN. When MLD snooping is enabled, a switch examines MLD 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 IPv6 multicast traffic only to those interfaces connected to interested receivers instead of flooding the traffic to all interfaces.

You can perform the following configurations for each VLAN:

- Selectively enable MLD snooping on specific VLANs.
- Specify the MLD version for the general query that the switch sends on an interface when the interface comes up.
- Enable immediate leave to reduce the length of time it takes the switch to stop forwarding multicast traffic when the last member host on the interface leaves the group.
- Configure an interface as a static multicast-router interface 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 MLD querier.

This topic covers:

- [Enabling or Disabling MLD Snooping on VLANs on page 55](#)
- [Configuring the MLD Version on page 56](#)
- [Enabling Immediate Leave on page 56](#)
- [Configuring an Interface as a Multicast-Router Interface on page 57](#)
- [Configuring Static Group Membership on an Interface on page 58](#)
- [Changing the Timer and Counter Values on page 59](#)

Enabling or Disabling MLD Snooping on VLANs

MLD snooping is not enabled on any VLAN by default. You must explicitly enable MLD snooping on specific interfaces.

- To enable MLD snooping on a specific VLAN:

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



NOTE: You cannot enable MLD snooping on a secondary VLAN.

For example, to enable MLD snooping on VLAN education:

```
[edit protocols mld-snooping]
user@switch# set vlan education
```

- To disable MLD snooping on a specific VLAN:

```
[edit protocols mld-snooping]
user@switch# delete vlan vlan-name
```

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

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

Configuring the MLD Version

You can configure the version of MLD queries sent by a switch when MLD snooping is enabled. By default, the switch uses MLD version 1 (MLDv1). If you are using Protocol-Independent Multicast source-specific multicast (PIM-SSM), we recommend that you configure the switch to use MLDv2.

Typically, a switch passively monitors MLD messages sent between multicast routers and hosts and does not send MLD queries. The exception is when a switch detects that an interface has come up. When an interface comes up, the switch sends an immediate general membership query to all hosts on the interface. By doing so, the switch enables the multicast routers to learn group memberships more quickly than they would if they had to wait until the MLD querier sent its next general query.

The MLD version of the general query determines the MLD version of the host membership reports as follows:

- MLD version 1 (MLDv1) general query—Both MLDv1 and MLDv2 hosts respond with an MLDv1 membership report.
- MLDv2 general query—MLDv2 hosts respond with an MLDv2 membership report, while MLDv1 hosts are unable to respond to the query.

By default, the switch sends MLDv1 queries. This ensures compatibility with hosts and multicast routers that support MLDv1 only and cannot process MLDv2 reports. However, if your VLAN contains MLDv2 multicast routers and hosts and the routers are running PIM-SSM, we recommend that you configure MLD snooping for MLDv2. Doing so enables the routers to quickly learn which multicast sources the hosts on the interface want to receive traffic from.



NOTE: Configuring the MLD version does not limit the version of MLD messages that the switch can snoop. A switch can snoop both MLDv1 and MLDv2 messages regardless of the MLD version configured.

To configure the MLD version on an interface:

```
[edit protocols]
user@switch# set mld interface interface-name version number
```

For example, to set the MLD version to version 2 on interface ge-0/0/2:

```
[edit protocols]
user@switch# set mld interface ge-0/0/2 version 2
```

Enabling Immediate Leave

By default, when a switch with MLD snooping enabled receives an MLD leave report on a member interface, it waits for hosts on the interface to respond to MLD 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, allowing the switch to keep track of the hosts on a 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 MLD version 1 (MLDv1) and MLDv2. However, with MLDv1, we recommend that you configure immediate leave only when there is only one MLD host on an interface. In MLDv1, only one host on a interface sends a membership report in response to a group-specific query—any other interested hosts suppress their reports. This report-suppression feature means that the switch only knows about one interested host at any given time.

To enable immediate leave on a VLAN:

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

Configuring an Interface as a Multicast-Router Interface

When MLD snooping is enabled on a switch, the switch determines which interfaces face a multicast router by monitoring interfaces for MLD queries or Protocol Independent Multicast (PIM) updates. 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 MLD snooping from reliably learning about a multicast-router interface through monitoring MLD queries or PIM updates.
- Your implementation does not require an MLD querier.
- You have a stable topology and want to avoid the delay the dynamic learning process entails.

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

```
[edit protocols]
user@switch# set mld-snooping vlan vlan-name interface interface-name
multicast-router-interface
```

For example, to configure ge-0/0/5.0 as a multicast-router interface for VLAN employee:

```
[edit protocols]
user@switch# set mld-snooping vlan employee 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 MLD 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 MLD membership reports as they arrive on interfaces on which MLD 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 MLD 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.

You cannot configure multicast source addresses for a static group interface. The MLD version of a static group interface is always MLD version 1.



NOTE: The switch does not simulate MLD 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 mld-snooping vlan vlan-name interface interface-name static group
ip-address
```

For example, to configure interface ge-0/0/11.0 in VLAN employee as a static member of multicast group ff1e::1:

```
[edit protocols]
user@switch# set mld-snooping vlan ip-camera-vlan interface ge-0/0/11.0 static group
ff1e::1
```

Changing the Timer and Counter Values

MLD uses various timers and counters to determine how often an MLD querier sends out membership queries and when group memberships time out. On Juniper Networks EX Series switches, the MLD and MLD snooping timers and counters default values are set to the values recommended in RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*. These values work well for most IPv6 multicast deployments.

There might be cases, however, where you might want to adjust 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 MLD 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.

The following timers and counters are configurable on a switch:

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

To configure the MLD query interval:

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

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

To configure the MLD query response interval:

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

- **query-last-member-interval**—The length of time the MLD querier waits between sending group-specific membership queries (the default is 1 second). The MLD 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 after the last member leaves a group.

To configure the MLD query last member interval:

```
[edit protocols]
user@switch# set mld-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 anticipated packet loss.

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

To configure **robust-count** for MLD snooping on a VLAN:

[edit protocols]

user@switch# set mld-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** value by the **robust-count** value and then adding the **query-response-interval** to the product:

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

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

$(125 \times 2) + 10 = 260$

To display the time remaining in the multicast listener interval before a group times out, use the **show mld-snooping membership** command.

**Related
Documentation**

- [Example: Configuring MLD Snooping on EX Series Switches on page 60](#)
- [Examples: Configuring MLD](#)
- [Verifying MLD Snooping on page 63](#)

Example: Configuring MLD Snooping on EX Series Switches



NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

You can enable MLD snooping on a VLAN to constrain the flooding of IPv6 multicast traffic on a VLAN. When MLD snooping is enabled, a switch examines MLD messages between hosts and multicast routers and learns which hosts are interested in receiving multicast traffic for a multicast group. On the basis of what it learns, the switch then forwards IPv6 multicast traffic only to those interfaces connected to interested receivers instead of flooding the traffic to all interfaces.

This example describes how to configure MLD snooping:

- [Requirements on page 61](#)
- [Overview and Topology on page 61](#)
- [Configuration on page 62](#)
- [Verifying MLD Snooping Configuration on page 63](#)

Requirements

This example uses the following software and hardware components:

- One EX Series switch running Junos OS with ELS
- Junos OS Release 13.3 or later for EX Series switches

Before you configure MLD snooping, be sure you have:

- Configured the vlan 100 VLAN 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.

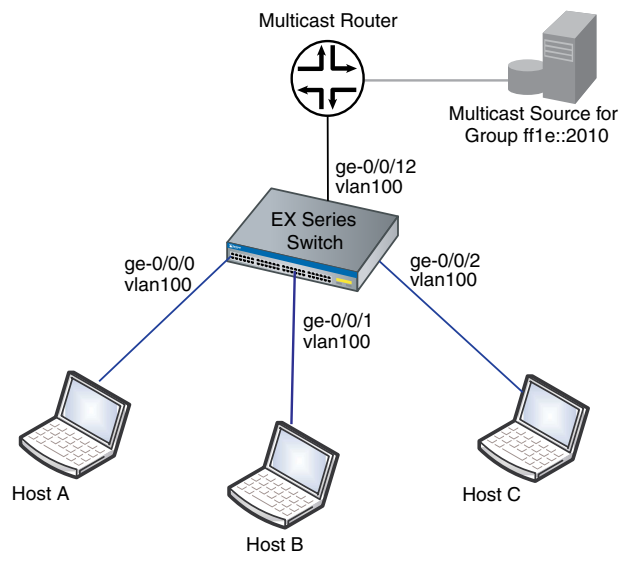
See *Configuring VLANs for EX Series Switches (CLI Procedure)*.

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 MLD querier and forwards multicast traffic for group ff1e::2010 to the switch from a multicast source.

The topology for this example is illustrated in [Figure 14 on page 61](#).

Figure 14: MLD Snooping Topology Example



In this sample topology, the multicast router forwards multicast traffic to the switch from the source when it receives a membership report for group ff1e::2010 from one of the hosts—for example, Host B. If MLD 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 MLD

snooping is enabled on vlan100, the switch monitors the MLD 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 enable MLD snooping on vlan100. It also 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 membership queries time out before it stops forwarding traffic.
- 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 MLD snooping on a switch:

CLI Quick Configuration

To quickly configure MLD snooping, copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols mld-snooping vlan vlan100
set protocols mld-snooping vlan vlan100 immediate-leave
set protocols mld-snooping vlan vlan100 interface ge-0/0/12 multicast-router-interface
```

Step-by-Step Procedure

To configure MLD snooping:

1. Enable MLD snooping on the VLAN vlan100:

```
[edit protocols]
user@switch# set mld-snooping vlan vlan100
```
2. 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 mld-snooping vlan vlan100 immediate-leave
```
3. Statically configure interface ge-0/0/12 as a multicast-router interface:

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

Results

Check the results of the configuration:

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


Verifying MLD Snooping Configuration

To verify that MLD snooping is enabled on the VLAN and the MLD snooping forwarding interfaces are correct, perform the following task:

- [Verifying MLD Snooping Interface Membership on VLAN vlan100 on page 63](#)

Verifying MLD Snooping Interface Membership on VLAN vlan100

Purpose Verify that MLD snooping is enabled on the VLAN vlan 100 and that the multicast-router interface is statically configured:

Action Show the MLD snooping information for ge-0/0/12.0:

```
user@switch> show mld snooping interface
Instance: default-switch
```

```
Vlan: vlan100
```

```
Learning-Domain: default
Interface: ge-0/0/12.0
  State:          Up Groups:      3
  Immediate leave: On
  Router interface: yes
```

```
Configured Parameters:
MLD Query Interval: 125.0
MLD Query Response Interval: 10.0
MLD Last Member Query Interval: 1.0
MLD Robustness Count: 2
```

Meaning MLD snooping is running on **vlan100**, and interface **ge-0/0/12.0** is a statically configured multicast-router interface. Immediate leave is enabled on the interface.

- Related Documentation**
- [Configuring MLD Snooping on a VLAN \(CLI Procedure\) on page 54](#)
 - [Verifying MLD Snooping on page 63](#)
 - [Understanding MLD Snooping on page 46](#)

Verifying MLD Snooping



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 *Verifying MLD Snooping (CLI Procedure)*. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

Multicast Listener Discovery (MLD) snooping constrains the flooding of IPv6 multicast traffic on VLANs. This topic describes how to verify MLD snooping operation on a VLAN.

It covers:

- [Verifying MLD Snooping Memberships on page 64](#)
- [Verifying MLD Snooping Interfaces on page 64](#)
- [Viewing MLD Snooping Statistics on page 65](#)
- [Viewing MLD Snooping Routing Information on page 66](#)

Verifying MLD Snooping Memberships

Purpose Verify that MLD snooping is enabled on a VLAN and determine group memberships.

Action Enter the following command:

```
user@switch> show mld snooping membership detail
Instance: default-switch
```

```
Vlan: v1
```

```
Learning-Domain: default
Interface: ge-0/0/1.0, Groups: 1
  Group: ff05::1
    Group mode: Exclude
    Source: ::
    Last reported by: fe80::
    Group timeout: 259 Type: Dynamic
Interface: ge-0/0/2.0, Groups: 0
```

Meaning The switch has multicast membership information for one VLAN on the switch, **v1**. MLD snooping might be enabled on other VLANs, but the switch does not have any multicast membership information for them.

- The following information is provided about the group memberships for the VLAN:
 - Currently, the VLAN has membership in only one multicast group, **ff05::1**.
 - The host or hosts that have reported membership in the group are on interface **ge-0/0/1.0**.
 - The last host that reported membership in the group has address **fe80::**.
 - The interface group membership will time out in **259** seconds if no hosts respond to membership queries during this interval.
 - The group membership has been learned by MLD snooping, as indicated by **Dynamic**.

Verifying MLD Snooping Interfaces

Purpose Display MLD snooping information for each interface on which MLD snooping is enabled.

Action Enter the following command:

```
user@switch> show mld snooping interface
Instance: default-switch
```

```
Vlan: v100
```

```

Learning-Domain: default
Interface: ge-0/0/1.0
  State:          Up Groups:      1
  Immediate leave: Off
  Router interface: no
Interface: ge-0/0/2.0
  State:          Up Groups:      0
  Immediate leave: Off
  Router interface: no

Configured Parameters:
MLD Query Interval: 125.0
MLD Query Response Interval: 10.0
MLD Last Member Query Interval: 1.0
MLD Robustness Count: 2

```

Meaning MLD snooping is configured on one VLAN on the switch, **v100**. Each interface in each VLAN is listed and the following information is provided:

- How many multicast groups the interface belongs to.
- Whether immediate leave has been configured for the interface.
- Whether the interface is a multicast-router interface.

The output also shows the configured parameters for the MLD querier.

Viewing MLD Snooping Statistics

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

Action Enter the following command:

```
user@switch>show mld snooping statistics
```

```

Vlan: v1
MLD Message type      Received      Sent  Rx errors
Listener Query (v1/v2)      0           4      0
Listener Report (v1)      447          0      0
Listener Done (v1/v2)      0           0      0
Listener Report (v2)       0           0      0
Other Unknown types                0

```

```

Vlan: v2
MLD Message type      Received      Sent  Rx errors
Listener Query (v1/v2)      0           4      0
Listener Report (v1)      154          0      0
Listener Done (v1/v2)      0           0      0
Listener Report (v2)       0           0      0
Other Unknown types                0

```

```

Instance: default-switch
MLD Message type      Received      Sent  Rx errors
Listener Query (v1/v2)      0           8      0
Listener Report (v1)      601          0      0
Listener Done (v1/v2)      0           0      0
Listener Report (v2)       0           0      0
Other Unknown types                0

```

MLD Global Statistics	
Bad Length	0
Bad Checksum	0
Bad Receive If	0
Rx non-local	0
Timed out	0

Meaning The output shows how many MLD messages of each type—**Queries**, **Done**, **Report**—the switch received or transmitted on interfaces on which MLD snooping is enabled. For each message type, it also shows the number of MLD packets the switch received that had errors—for example, packets that do not conform to the MLDv1 or MLDv2 standards. If the **Rx errors** count increases, verify that the hosts are compliant with MLDv1 or MLDv2 standards. If the switch is unable to recognize the MLD message type for a packet, it counts the packet under **Other Unknown types**.

Viewing MLD Snooping Routing Information

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

Action Enter the following command:

```
user@switch>show multicast snooping route
Nexthop Bulking: OFF
```

```
Family: INET6
```

```
Group: ff00::/8
Source: ::/128
Vlan: v1

Group: ff02::1/128
Source: ::/128
Vlan: v1
Downstream interface list:
ge-1/0/16.0
```

```
Group: ff05::1/128
Source: ::/128
Vlan: v1
Downstream interface list:
ge-1/0/16.0
```

```
Group: ff06::1/128
Source: ::/128
Vlan: v1
Downstream interface list:
ge-1/0/16.0
```

Meaning The output shows the next-hop interfaces for a given multicast group on a VLAN. For example, route **ff02::1/128** on VLAN **v1** has the next-hop interface **ge-1/0/16.0**.

Related Documentation

- [clear mld snooping membership on page 448](#)
- [clear mld snooping statistics on page 449](#)
- [Example: Configuring MLD Snooping on EX Series Switches on page 60](#)

- [Configuring MLD Snooping on a VLAN \(CLI Procedure\) on page 54](#)

Configuring MLD Snooping Tracing Operations (CLI Procedure)

By enabling tracing operations for MLD snooping, you can record detailed messages about the operation of the protocol, such as the various types of protocol packets sent and received. [Table 5 on page 67](#) describes the tracing operations you can enable and the flags used to specify them in the tracing configuration.

Table 5: Supported Tracing Operations for MLD Snooping

Tracing Operation	Flag
Trace all (equivalent of including all flags).	all
Trace client notifications.	client-notification
Trace general MLD snooping protocol events.	general
Trace group operations.	group
Trace host notifications.	host-notification
Trace leave reports.	leave
Trace normal MLD snooping protocol events. If you do not specify this flag, only unusual or abnormal operations are traced.	normal
Trace all MLD packets.	packets
Trace policy processing.	policy
Trace MLD 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

This topic covers:

- [Configuring Tracing Operations on page 68](#)
- [Viewing, Stopping, and Restarting Tracing Operations on page 68](#)

Configuring Tracing Operations

To configure tracing operations for MLD snooping:

1. Configure the filename for the trace file:

```
[edit protocols mld-snooping ]
user@switch# set vlan vlan-name traceoptions file filename
```

For example:

```
[edit protocols mld-snooping ]
user@switch# set vlan vlan100 traceoptions file mld-snoop-trace
```

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

```
[edit protocols mld-snooping ]
user@switch # set vlan vlan-name traceoptions file files number size size
```

For example:

```
[edit protocols mld-snooping ]
user@switch # set vlan vlan100 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, and the maximum file size to 128 KB.

3. Specify one of the tracing flags shown in [Table 5 on page 67](#):

```
[edit protocols mld-snooping ]
user@switch # set vlan vlan-name traceoptions flag flagname
```

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

```
[edit protocols mld-snooping ]
user@switch# set vlan vlan100 traceoptions flag vlan

[edit protocols mld-snooping ]
user@switch# set vlan vlan100 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/mld-snoop-trace
```

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

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

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

- Related Documentation**
- *Configuring MLD Snooping on a VLAN (CLI Procedure)*
 - [Configuring MLD Snooping on a VLAN \(CLI Procedure\) on page 54](#)
 - *Tracing and Logging Junos OS Operations*

PART 3

Configuring Protocol Independent Multicast

- [Understanding PIM on page 73](#)
- [Configuring PIM Basics on page 77](#)
- [Routing Content to Densely Clustered Receivers with PIM Dense Mode on page 93](#)
- [Routing Content to Larger, Sparser Groups with PIM Sparse Mode on page 99](#)
- [Rapidly Detecting Communication Failures with PIM and BFD Protocol on page 131](#)

CHAPTER 4

Understanding PIM

- [PIM Overview on page 73](#)

PIM Overview

The predominant multicast routing protocol in use on the Internet today is Protocol Independent Multicast, or PIM. The type of PIM used on the Internet is PIM sparse mode. PIM sparse mode is so accepted that when the simple term “PIM” is used in an Internet context, some form of sparse mode operation is assumed.

PIM emerged as an algorithm to overcome the limitations of dense-mode protocols such as the Distance Vector Multicast Routing Protocol (DVMRP), which was efficient for dense clusters of multicast receivers, but did not scale well for the larger, sparser, groups encountered on the Internet. The Core Based Trees (CBT) Protocol was intended to support sparse mode as well, but CBT, with its all-powerful core approach, made placement of the core critical, and large conference-type applications (many-to-many) resulted in bottlenecks in the core. PIM was designed to avoid the dense-mode scaling issues of DVMRP and the potential performance issues of CBT at the same time.

PIM is one of the most rapidly evolving specifications on the Internet today. Since its introduction in 1995, PIM has already seen two major revisions to its packet structure (PIM version 1 [PIMv1] and PIM version 2 [PIMv2]), two major RFCs (RFC 2362 obsoleted RFC 2117), and numerous drafts describing major components of PIM, such as many-to-many trees and source-specific multicast (SSM). Long-lasting RFCs are not a feature of PIM, and virtually all of PIM must be researched, understood, and implemented directly from Internet drafts. In fact, no current RFC describes PIMv1 at all. The drafts have all expired, and PIMv1 was never issued as an official RFC.

PIM itself is not nonstandard or unstable, however. PIM has been a promising multicast routing protocol since its inception, especially PIM sparse mode, the first real sparse-mode multicast routing protocol. Work continues on PIM in a number of areas, from bidirectional trees to network management, and the rapid pace of development makes drafts essential for PIM.

PIMv1 and PIMv2 can coexist on the same routing device and even on the same interface. The main difference between PIMv1 and PIMv2 is the packet format. PIMv1 messages use Internet Group Management Protocol (IGMP) packets, whereas PIMv2 has its own IP protocol number (103) and packet structure. All routing devices connecting to an IP subnet such as a LAN must use the same PIM version. Some PIM implementations can

recognize PIMv1 packets and automatically switch the routing device interface to PIMv1. Because the difference between PIMv1 and PIMv2 involves the message format, but not the meaning of the message or how the routing device processes the PIM message, a routing device can easily mix PIMv1 and PIMv2 interfaces.

PIM is used for efficient routing to multicast groups that might span wide-area and interdomain internetworks. It is called “protocol independent” because it does not depend on a particular unicast routing protocol. Junos OS supports bidirectional mode, sparse mode, dense mode, and sparse-dense mode.

PIM operates in several modes: bidirectional mode, sparse mode, dense mode, and sparse-dense mode. In sparse-dense mode, some multicast groups are configured as dense mode (flood-and-prune, [S,G] state) and others are configured as sparse mode (explicit join to rendezvous point [RP], [*G] state).

PIM drafts also establish a mode known as PIM source-specific mode, or PIM SSM. In PIM SSM there is only one specific source for the content of a multicast group within a given domain.

Because the PIM mode you choose determines the PIM configuration properties, you first must decide whether PIM operates in bidirectional, sparse, dense, or sparse-dense mode in your network. Each mode has distinct operating advantages in different network environments.

- In sparse mode, routing devices must join and leave multicast groups explicitly. Upstream routing devices do not forward multicast traffic to a downstream routing device unless the downstream routing device has sent an explicit request (by means of a join message) to the rendezvous point (RP) routing device to receive this traffic. The RP serves as the root of the shared multicast delivery tree and is responsible for forwarding multicast data from different sources to the receivers.

Sparse mode is well suited to the Internet, where frequent interdomain join messages and prune messages are common.



NOTE: On all the EX series switches (except EX4300 and EX9200), QFX5100 switches, and OCX series switches, the rate limit is set to 1pps per SG to avoid overwhelming the rendezvous point (RP), First hop router (FHR) with PIM-sparse mode (PIM-SM) register messages and cause CPU hogs. This rate limit helps in improving scaling and convergence times by avoiding duplicate packets being trapped, and tunneled to RP in software.

- Bidirectional PIM is similar to sparse mode, and is especially suited to applications that must scale to support a large number of dispersed sources and receivers. In bidirectional PIM, routing devices build shared bidirectional trees and do not switch to a source-based tree. Bidirectional PIM scales well because it needs no source-specific (S,G) state. Instead, it builds only group-specific (*G) state.
- Unlike sparse mode and bidirectional mode, in which data is forwarded only to routing devices sending an explicit PIM join request, dense mode implements a *flood-and-prune* mechanism, similar to the Distance Vector Multicast Routing Protocol (DVMRP). In

dense mode, a routing device receives the multicast data on the incoming interface, then forwards the traffic to the outgoing interface list. Flooding occurs periodically and is used to refresh state information, such as the source IP address and multicast group pair. If the routing device has no interested receivers for the data, and the outgoing interface list becomes empty, the routing device sends a PIM prune message upstream.

Dense mode works best in networks where few or no prunes occur. In such instances, dense mode is actually more efficient than sparse mode.

- Sparse-dense mode, as the name implies, 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 an RP. Instead, data packets destined for that group are forwarded by means of PIM dense mode rules. A group specified as “sparse” is mapped to an RP, and data packets are forwarded by means of PIM sparse-mode rules. Sparse-dense mode is useful in networks implementing auto-RP for PIM sparse mode.

Basic PIM Network Components

PIM dense mode requires only a multicast source and series of multicast-enabled routing devices running PIM dense mode to allow receivers to obtain multicast content. Dense mode makes sure that all multicast traffic gets everywhere by periodically flooding the network with multicast traffic, and relies on prune messages to make sure that subnets where all receivers are uninterested in that particular multicast group stop receiving packets.

PIM sparse mode is more complicated and requires the establishment of special routing devices called *rendezvous points (RPs)* in the network core. These routing devices are where upstream join messages from interested receivers meet downstream traffic from the source of the multicast group content. A network can have many RPs, but PIM sparse mode allows only one RP to be active for any multicast group.

If there is only one RP in a routing domain, the RP and adjacent links might become congested and form a single point of failure for all multicast traffic. Thus, multiple RPs are the rule, but the issue then becomes how other multicast routing devices find the RP that is the source of the multicast group the receiver is trying to join. This RP-to-group mapping is controlled by a special *bootstrap router (BSR)* running the PIM BSR mechanism. There can be more than one bootstrap router as well, also for single-point-of-failure reasons.

The bootstrap router does not have to be an RP itself, although this is a common implementation. The bootstrap router's main function is to manage the collection of RPs and allow interested receivers to find the source of their group's multicast traffic. PIM bootstrap messages are sourced from the loopback address, which is always up. The loopback address must be routable. If it is not routable, then the bootstrap router is unable to send bootstrap messages to update the RP domain members. The **show pim bootstrap** command displays only those bootstrap routers that have routable loopback addresses.

PIM SSM can be seen as a subset of a special case of PIM sparse mode and requires no specialized equipment other than that used for PIM sparse mode (and IGMP version 3).

Bidirectional PIM RPs, unlike RPs for PIM sparse mode, do not need to perform PIM Register tunneling or other specific protocol action. Bidirectional PIM RPs implement no specific functionality. RP addresses are simply a location in the network to rendezvous toward. In fact, for bidirectional PIM, RP addresses need not be loopback interface addresses or even be addresses configured on any routing device, as long as they are covered by a subnet that is connected to a bidirectional PIM-capable routing device and advertised to the network.

- Related Documentation**
- [Supported IP Multicast Protocol Standards on page 15](#) in the *Multicast Protocols Feature Guide for Routing Devices*

CHAPTER 5

Configuring PIM Basics

- [Configuring Basic PIM Settings on page 77](#)
- [Configuring Multiple Instances of PIM on page 89](#)
- [Configuring a Designated Router for PIM on page 90](#)

Configuring Basic PIM Settings

- [PIM Configuration Statements on page 77](#)
- [Changing the PIM Version on page 80](#)
- [Modifying the PIM Hello Interval on page 80](#)
- [Preserving Multicast Performance by Disabling Response to the ping Utility on page 81](#)
- [PIM on Aggregated Interfaces on page 82](#)
- [Configuring PIM Trace Options on page 82](#)
- [Disabling PIM on page 84](#)
- [Verifying a Multicast Configuration on page 87](#)

PIM Configuration Statements

To configure Protocol Independent Multicast (PIM), include the **pim** statement:

```
pim {  
  disable;  
  default-vpn-source {  
    interface-name interface-name;  
  }  
  assert-timeout seconds;  
  dense-groups {  
    addresses;  
  }  
  dr-election-on-p2p;  
  export;  
  graceful-restart {  
    disable;  
    no-bidirectional-mode;  
    restart-duration seconds;  
  }  
  idle-standby-path-switchover-delay seconds;  
  import [ policy-names ];
```

```

interface interface-name {
  bidirectional {
    df-election {
      backoff-period milliseconds;
      offer-period milliseconds;
      robustness-count number;
    }
  }
  import;
  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 {
  automatic;
}
join-prune-timeout;
nonstop-routing {
  disable;
}
override-interval milliseconds;
propagation-delay milliseconds;
reset-tracking-bit;
rib-group {
  inet group-name;
  inet6 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-export [ policy-names ];
  bootstrap-import [ policy-names ];
}

```



```

bootstrap-priority number;
dr-register-policy [ policy-names ];
embedded-rp {
    group-ranges {
        destination-ip-prefix </prefix-length>;
    }
    maximum-rps limit;
}
local {
    family (inet | inet6) {
        address address;
        anycast-pim {
            rp-set {
                address address <forward-msdp-sa>;
            }
            local-address address;
        }
        disable;
        group-ranges {
            destination-ip-prefix </prefix-length>;
        }
        hold-time seconds;
        override;
        priority number;
    }
}
rp-register-policy [ policy-names ];
standby-path-creation-delay seconds;
static {
    address address {
        override;
        version version;
        group-ranges {
            destination-ip-prefix </prefix-length>;
        }
        spt-threshold {
            infinity [ policy-names ];
        }
        traceoptions {
            file filename <files number> <size size> <world-readable | no-world-readable>;
            flag flag <flag-modifier> <disable>;
        }
    }
}
}
}

```

You can include this statement at the following hierarchy levels:

- [edit protocols]
- [edit routing-instances *routing-instance-name* protocols]
- [edit logical-systems *logical-system-name* protocols]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols]

By default, PIM is disabled.



NOTE: You cannot configure PIM within a nonforwarding instance. If you try to do so, the router displays a commit check error and does not complete the configuration commit process.

Changing the PIM Version

All systems on a subnet must run the same version of PIM.

The default PIM version can be version 1 or version 2, depending on the mode you are configuring. PIMv1 is the default for rendezvous point (RP) mode (at the **[edit protocols pim rp static address address]** hierarchy level). However, PIMv2 is the default for interface mode (at the **[edit protocols pim interface interface-name]** hierarchy level). Explicitly configured versions override the defaults.

To configure the PIM version, include the **version** statement:

```
version (1 | 2);
```

Modifying the PIM Hello Interval

Routing devices send hello messages at a fixed interval on all PIM-enabled interfaces. By using hello messages, routing devices advertise their existence as PIM routing devices on the subnet. With all PIM-enabled routing devices advertised, a single designated router for the subnet is established.

When a routing device is configured for PIM, it sends a hello message at a 30-second default interval. The interval range is from 0 through 255. When the interval counts down to 0, the routing device sends another hello message, and the timer is reset. A routing device that receives no response from a neighbor in 3.5 times the interval value drops the neighbor. In the case of a 30-second interval, the amount of time a routing device waits for a response is 105 seconds.

If a PIM hello message contains the hold-time option, the neighbor timeout is set to the hold-time sent in the message. If a PIM hello message does not contain the hold-time option, the neighbor timeout is set to the default hello hold time.

To modify how often the routing device sends hello messages out of an interface:

1. This example shows the configuration for the routing instance. Configure the interface globally or in the routing instance.

```
[edit routing-instances PIM.master protocols pim interface fe-3/0/2.0]
user@host# set hello-interval 255
```

2. Verify the configuration by checking the **Hello Option Holdtime** field in the output of the **show pim neighbors detail** command.

```
user@host> show pim neighbors detail
Instance: PIM.master
Interface: fe-3/0/2.0
Address: 192.168.195.37, IPv4, PIM v2, Mode: Sparse
```

```

Hello Option Holdtime: 255 seconds
Hello Option DR Priority: 1
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Join Suppression supported
Rx Join: Group Source Timeout
225.1.1.1 192.168.195.78 0
225.1.1.1 0

```

```

Interface: lo0.0
Address: 10.255.245.91, IPv4, PIM v2, Mode: Sparse
Hello Option Holdtime: 255 seconds
Hello Option DR Priority: 1
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Join Suppression supported

```

```

Interface: pd-6/0/0.32768
Address: 0.0.0.0, IPv4, PIM v2, Mode: Sparse
Hello Option Holdtime: 255 seconds
Hello Option DR Priority: 0
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Join Suppression supported

```

Preserving Multicast Performance by Disabling Response to the ping Utility

The ping utility uses ICMP Echo messages to verify connectivity to any device with an IP address. However, in the case of multicast applications, a single ping sent to a multicast address can degrade the performance of routers because the stream of packets is replicated multiple times.

You can disable the router's response to ping (ICMP Echo) packets sent to multicast addresses. The system responds normally to unicast ping packets.

To disable the router's response to ping packets sent to multicast addresses:

1. Include the **no-multicast-echo** statement:

```

[edit system]
user@host# set no-multicast-echo

```

2. Verify the configuration by checking the **echo drops with broadcast or multicast destination address** field in the output of the **show system statistics icmp** command.

```

user@host> show system statistics icmp

icmp:
0 drops due to rate limit
0 calls to icmp_error
0 errors not generated because old message was icmp
Output histogram:
echo reply: 21
0 messages with bad code fields
0 messages less than the minimum length
0 messages with bad checksum
0 messages with bad source address
0 messages with bad length
100 echo drops with broadcast or multicast destination address
0 timestamp drops with broadcast or multicast destination address
Input histogram:
echo: 21
21 message responses generated

```

PIM on Aggregated Interfaces

You can configure several Protocol Independent Multicast (PIM) features on an interface regardless of its PIM mode (bidirectional, sparse, dense, or sparse-dense mode).

If you configure PIM on an aggregated (**ae-** or **as-**) interface, each of the interfaces in the aggregate is included in the multicast output interface list and carries the single stream of replicated packets in a load-sharing fashion. The multicast aggregate interface is “expanded” into its constituent interfaces in the next-hop database.



NOTE: For Draft Rosen multicast VPNs (MVPNs) load balancing over aggregated Ethernet interfaces is uneven. In the case of Next-Generation MBGP MPVNs, multicast traffic is sent over point-to-multipoint and RSVP, and the hash is computed up to the IP headers. In the Draft Rosen case, multicast traffic is tunneled over GRE tunnels, and the hash is used only on GRE tunnel headers. This is why load balancing is not even for Draft Rosen, even when the LAGs are all core interfaces.

Configuring PIM Trace Options

Tracing operations record detailed messages about the operation of routing protocols, such as the various types of routing protocol packets sent and received, and routing policy actions. You can specify which trace operations are logged by including specific tracing flags. The following table describes the flags that you can include.

Flag	Description
all	Trace all operations.
assert	Trace assert messages, which are used to resolve which of the parallel routers connected to a multiaccess LAN is responsible for forwarding packets to the LAN.
autorp	Trace bootstrap, RP, and auto-RP messages.
bidirectional-df-election	Trace bidirectional PIM designated-forwarder (DF) election events.
bootstrap	Trace bootstrap messages, which are sent periodically by the PIM domain's bootstrap router and are forwarded, hop by hop, to all routers in that domain.
general	Trace general events.
graft	Trace graft and graft acknowledgment messages.
hello	Trace hello packets, which are sent so that neighboring routers can discover one another.

Flag	Description
join	Trace join messages, which are sent to join a branch onto the multicast distribution tree.
mdt	Trace messages related to multicast data tunnels.
normal	Trace normal events.
nsr-synchronization	Trace nonstop routing synchronization events
packets	Trace all PIM packets.
policy	Trace poison-route-reverse packets.
prune	Trace prune messages, which are sent to prune a branch off the multicast distribution tree.
register	Trace register and register-stop messages. Register messages are sent to the RP when a multicast source first starts sending to a group.
route	Trace routing information.
rp	Trace candidate RP advertisements.
state	Trace state transitions.
task	Trace task processing.
timer	Trace timer processing.

In the following example, tracing is enabled for all routing protocol packets. Then tracing is narrowed to focus only on PIM packets of a particular type.

To configure tracing operations for PIM:

1. (Optional) Configure tracing at the [**routing-options** hierarchy level to trace all protocol packets.

```
[edit routing-options traceoptions]
user@host# set file all-packets-trace
user@host# set flag all
```

2. Configure the filename for the PIM trace file.

```
[edit protocols pim traceoptions]
user@host# set file pim-trace
```

3. (Optional) Configure the maximum number of trace files.

```
[edit protocols pim traceoptions]
user@host# set file files 5
```

4. (Optional) Configure the maximum size of each trace file.

```
[edit protocols pim traceoptions]  
user@host# set file size 1m
```

5. (Optional) Enable unrestricted file access.

```
[edit protocols pim traceoptions]  
user@host# set file world-readable
```

6. Configure tracing flags.

Suppose you are troubleshooting issues with PIM version 1 control packets that are received on an interface configured for PIM version 2. The following example shows how to trace messages associated with this problem.

```
[edit protocols pim traceoptions]  
user@host# set flag packets | match "Rx V1 Require V2"
```

7. View the trace file.

```
user@host> file list /var/log  
user@host> file show /var/log/pim-trace
```

Disabling PIM

By default, when configured, the PIM protocol is enabled on all interfaces for all families. If desired, you can disable PIM at the protocol, interface, or family hierarchy levels.

The hierarchy in which you configure PIM is critical. In general, the most specific configuration takes precedence. However, if PIM is disabled at the protocol level, then any disable statements with respect to an interface or family are ignored.

For example, the order of precedence for disabling PIM on a particular interface family is:

1. If PIM is disabled at the **[edit protocols pim interface *interface-name* family]** hierarchy level, then PIM is disabled for that interface family.
2. If PIM is not configured at the **[edit protocols pim interface *interface-name* family]** hierarchy level, but is disabled at the **[edit protocols pim interface *interface-name*]** hierarchy level, then PIM is disabled for all families on the specified interface.
3. If PIM is not configured at either the **[edit protocols pim interface *interface-name* family]** hierarchy level or the **[edit protocols pim interface *interface-name*]** hierarchy level, but is disabled at the **[edit protocols pim]** hierarchy level, then the PIM protocol is disabled globally for all interfaces and all families.

The following sections describe how to disable PIM at the various hierarchy levels.

- [Disabling the PIM Protocol on page 85](#)
- [Disabling PIM on an Interface on page 85](#)
- [Disabling PIM for a Family on page 86](#)
- [Disabling PIM for a Rendezvous Point on page 86](#)

Disabling the PIM Protocol

You can explicitly disable the PIM protocol. Disabling the PIM protocol disables the protocol for all interfaces and all families. This is accomplished at the **[edit protocols pim]** hierarchy level:

```
[edit protocols]
pim {
  disable;
}
```

To disable the PIM protocol:

1. Include the **disable** statement.

```
user@host# set protocols pim disable
```

2. (Optional) Verify your configuration settings before committing them by using the **show protocols pim** command.

```
user@host# run show protocols pim
```

Disabling PIM on an Interface

You can disable the PIM protocol on a per-interface basis. This is accomplished at the **[edit protocols pim interface *interface-name*]** hierarchy level:

```
[edit protocols]
pim {
  interface interface-name {
    disable;
  }
}
```

To disable PIM on an interface:

1. Include the **disable** statement.

```
user@host# set protocols pim interface fe-0/1/0 disable
```

2. (Optional) Verify your configuration settings before committing them by using the **show protocols pim** command.

```
user@host# run show protocols pim
```

Disabling PIM for a Family

You can disable the PIM protocol on a per-family basis. This is accomplished at the **[edit protocols pim family]** hierarchy level:

```
[edit protocols]
pim {
  family inet {
    disable;
  }
  family inet6 {
    disable;
  }
}
```

To disable PIM for a family:

1. Include the **disable** statement.

```
user@host# set protocols pim family inet disable
user@host# set protocols pim family inet6 disable
```

2. (Optional) Verify your configuration settings before committing them by using the **show protocols pim** command.

```
user@host# run show protocols pim
```

Disabling PIM for a Rendezvous Point

You can disable the PIM protocol for a rendezvous point (RP) on a per-family basis. This is accomplished at the **[edit protocols pim rp local family]** hierarchy level:

```
[edit protocols]
pim {
  rp {
    local {
      family inet {
        disable;
      }
      family inet6 {
        disable;
      }
    }
  }
}
```

To disable PIM for an RP family:

1. Use the **disable** statement.

```
user@host# set protocols pim rp local family inet disable
user@host# set protocols pim rp local family inet6 disable
```

2. (Optional) Verify your configuration settings before committing them by using the **show protocols pim** command.

```
user@host# run show protocols pim
```


Verifying a Multicast Configuration

To verify a multicast configuration, perform these tasks:

- [Verifying SAP and SDP Addresses and Ports on page 87](#)
- [Verifying the IGMP Version on page 87](#)
- [Verifying the PIM Mode and Interface Configuration on page 88](#)
- [Verifying the PIM RP Configuration on page 88](#)
- [Verifying the RPF Routing Table Configuration on page 88](#)

Verifying SAP and SDP Addresses and Ports

Purpose Verify that SAP and SDP are configured to listen on the correct group addresses and ports.

Action From the CLI, enter the **show sap listen** command.

Sample Output

```
user@host> show sap listen
Group Address  Port
224.2.127.254  9875
```

Meaning The output shows a list of the group addresses and ports that SAP and SDP listen on. Verify the following information:

- Each group address configured, especially the default **224.2.127.254**, is listed.
- Each port configured, especially the default **9875**, is listed.

Verifying the IGMP Version

Purpose Verify that IGMP version 2 is configured on all applicable interfaces.

Action From the CLI, enter the **show igmp interface** command.

Sample Output

```
user@host> show igmp interface
Interface: ge-0/0/0.0
  Querier: 192.168.4.36
  State:          Up Timeout:      197 Version:  2 Groups:      0

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
```

Meaning The output shows a list of the interfaces that are configured for IGMP. Verify the following information:

- Each interface on which IGMP is enabled is listed.
- Next to **Version**, the number 2 appears.

Verifying the PIM Mode and Interface Configuration

Purpose Verify that PIM sparse mode is configured on all applicable interfaces.

Action From the CLI, enter the **show pim interfaces** command.

Sample Output

```
user@host> show pim interfaces
Instance: PIM.master
Name           Stat Mode      IP V State Count DR address
1o0.0           Up  Sparse    4 2 DR        0 127.0.0.1
pim.32769       Up  Sparse    4 2 P2P        0
```

Meaning The output shows a list of the interfaces that are configured for PIM. Verify the following information:

- Each interface on which PIM is enabled is listed.
- The network management interface, either **ge-0/0/0** or **fe-0/0/0**, is *not* listed.
- Under **Mode**, the word **Sparse** appears.

Verifying the PIM RP Configuration

Purpose Verify that the PIM RP is statically configured with the correct IP address.

Action From the CLI, enter the **show pim rps** command.

Sample Output

```
user@host> show pim rps
Instance: PIM.master
Address family INET
RP address      Type      Holdtime Timeout Active groups Group prefixes
192.168.14.27   static    0         None      2 224.0.0.0/4
```

Meaning The output shows a list of the RP addresses that are configured for PIM. At least one RP must be configured. Verify the following information:

- The configured RP is listed with the proper IP address.
- Under **Type**, the word **static** appears.

Verifying the RPF Routing Table Configuration

Purpose Verify that the PIM RPF routing table is configured correctly.

Action From the CLI, enter the **show multicast rpf** command.

Sample Output

```
user@host> show multicast rpf
Multicast RPF table: inet.0 , 2 entries...
```

Meaning The output shows the multicast RPF table that is configured for PIM. If no multicast RPF routing table is configured, RPF checks use **inet.0**. Verify the following information:

- The configured multicast RPF routing table is **inet.0**.
- The **inet.0** table contains entries.

Related Documentation

- [Configuring PIM Auto-RP on page 99](#)
- [Configuring PIM Bootstrap Router on page 113](#)
- [Configuring PIM Dense Mode on page 93](#)
- [Configuring a Designated Router for PIM on page 90](#)
- [Configuring PIM Filtering on page 117](#)
- [Configuring PIM Sparse-Dense Mode on page 96](#)
- [Configuring PIM and the Bidirectional Forwarding Detection \(BFD\) Protocol on page 131](#)
- *Example: Configuring Nonstop Active Routing for PIM*
- *Examples: Configuring PIM RPT and SPT Cutover*
- *Examples: Configuring PIM Sparse Mode*
- [Configuring PIM Sparse-Dense Mode on page 96](#)
- [Configuring PIM and the Bidirectional Forwarding Detection \(BFD\) Protocol on page 131](#)

Configuring Multiple Instances of PIM

PIM instances are supported only for VRF instance types. You can configure multiple instances of PIM to support multicast over VPNs.

To configure multiple instances of PIM, include the following statements:

```
routing-instances {
  routing-instance-name {
    interface interface-name;
    instance-type vrf;
    protocols {
      pim {
        ... pim-configuration ...
      }
    }
  }
}
```

You can include the statements at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols]

**Related
Documentation**

- *Multicast Protocols Feature Guide for Routing Devices*
- *Junos OS VPNs Library for Routing Devices*

Configuring a Designated Router for PIM

- [Configuring Interface Priority for PIM Designated Router Selection on page 90](#)
- [Configuring PIM Designated Router Election on Point-to-Point Links on page 91](#)

Configuring Interface Priority for PIM Designated Router Selection

A designated router (DR) sends periodic join messages and prune messages toward a group-specific rendezvous point (RP) for each group for which it has active members. When a Protocol Independent Multicast (PIM) router learns about a source, it originates a Multicast Source Discovery Protocol (MSDP) source-address message if it is the DR on the upstream interface.

By default, every PIM interface has an equal probability (priority 1) of being selected as the DR. Configuring the interface DR priority helps ensure that changing an IP address does not alter your forwarding model.

To configure the interface designated router priority:

1. This example shows the configuration for the routing instance. Configure the interface globally or in the routing instance.

```
[edit routing-instances PIM.master protocols pim interface ge-0/0/0.0 family inet]
user@host# set priority 5
```

2. Verify the configuration by checking the **Hello Option DR Priority** field in the output of the **show pim neighbors detail** command.

```
user@host> show pim neighbors detail

Instance: PIM.master
Interface: ge-0/0/0.0
Address: 192.168.195.37, IPv4, PIM v2, Mode: Sparse
Hello Option Holdtime: 65535 seconds
Hello Option DR Priority: 5
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Join Suppression supported
Rx Join: Group Source Timeout
225.1.1.1 192.168.195.78 0
225.1.1.1 0

Interface: lo0.0
Address: 10.255.245.91, IPv4, PIM v2, Mode: Sparse
Hello Option Holdtime: 65535 seconds
Hello Option DR Priority: 1
```

```
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Join Suppression supported
```

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

Configuring PIM Designated Router Election on Point-to-Point Links

To comply with the latest PIM drafts, enable designated router (DR) election on all PIM interfaces, including point-to-point (P2P) interfaces. (DR election is enabled by default on all other interfaces.) One of the two routers might join a multicast group on its P2P link interface. The DR on that link is responsible for initiating the relevant join messages.

To enable DR election on point-to-point interfaces:

1. On both point-to-point link routers, configure the router globally or in the routing instance. This example shows the configuration for the routing instance.

```
[edit routing-instances PIM.master protocols pim]
user@host# set dr-election-on-p2p
```

2. Verify the configuration by checking the **State** field in the output of the **show pim interfaces** command. The possible values for the **State** field are DR, NotDR, and P2P. When a point-to-point link interface is elected to be the DR, the interface state becomes DR instead of P2P.
3. If the **show pim interfaces** command continues to report the P2P state, consider running the **restart routing** command on both routers on the point-to-point link. Then recheck the state.



CAUTION: Do not restart a software process unless specifically asked to do so by your Juniper Networks customer support representative. Restarting a software process during normal operation of a routing platform could cause interruption of packet forwarding and loss of data.

```
[edit]
user@host# run restart routing
```

Related Documentation

- [Configuring PIM Auto-RP on page 99](#)
- [Configuring PIM Bootstrap Router on page 113](#)
- [Configuring PIM Dense Mode on page 93](#)
- [Configuring PIM Filtering on page 117](#)
- [Example: Configuring Nonstop Active Routing for PIM](#)
- [Examples: Configuring PIM RPT and SPT Cutover](#)
- [Examples: Configuring PIM Sparse Mode](#)

- [Configuring PIM Sparse-Dense Mode on page 96](#)
- [Configuring PIM and the Bidirectional Forwarding Detection \(BFD\) Protocol on page 131](#)
- [Configuring Basic PIM Settings on page 77](#)

CHAPTER 6

Routing Content to Densely Clustered Receivers with PIM Dense Mode

- [Configuring PIM Dense Mode on page 93](#)
- [Configuring PIM Sparse-Dense Mode on page 96](#)

Configuring PIM Dense Mode

- [Understanding PIM Dense Mode on page 93](#)
- [Configuring PIM Dense Mode Properties on page 95](#)

Understanding PIM Dense Mode

PIM dense mode is less sophisticated than PIM sparse mode. PIM dense mode is useful for multicast LAN applications, the main environment for all dense mode protocols.

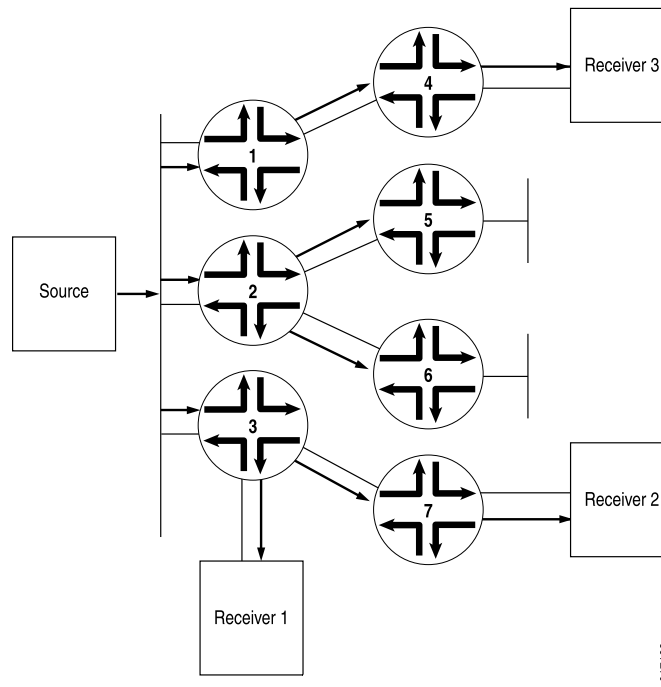
PIM dense mode implements the same flood-and-prune mechanism that DVMRP and other dense mode routing protocols employ. The main difference between DVMRP and PIM dense mode is that PIM dense mode introduces the concept of protocol independence. PIM dense mode can use the routing table populated by any underlying unicast routing protocol to perform reverse-path-forwarding (RPF) checks.

Internet service providers (ISPs) typically appreciate the ability to use any underlying unicast routing protocol with PIM dense mode because they do not need to introduce and manage a separate routing protocol just for RPF checks. While unicast routing protocols extended as multiprotocol BGP (MBGP) and Multitopology Routing in IS-IS (M-IS-IS) were later employed to build special tables to perform RPF checks, PIM dense mode does not require them.

PIM dense mode can use the unicast routing table populated by OSPF, IS-IS, BGP, and so on, or PIM dense mode can be configured to use a special multicast RPF table populated by MBGP or M-IS-IS when performing RPF checks.

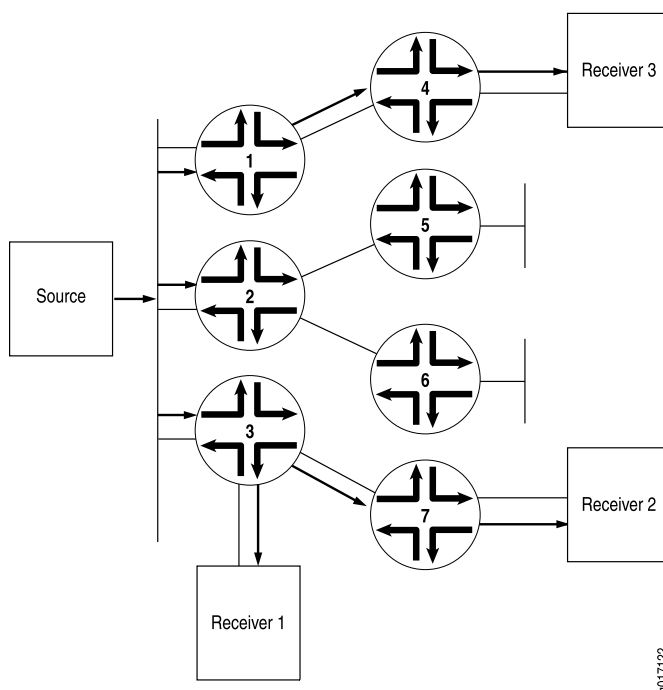
Unlike sparse mode, in which data is forwarded only to routers sending an explicit request, dense mode implements a *flood-and-prune* mechanism, similar to DVMRP. In PIM dense mode, there is no RP. A router receives the multicast data on the interface closest to the source, then forwards the traffic to all other interfaces (see [Figure 15 on page 94](#)).

Figure 15: Multicast Traffic Flooded from the Source Using PIM Dense Mode



Flooding occurs periodically. It is used to refresh state information, such as the source IP address and multicast group pair. If the router has no interested receivers for the data, and the OIL becomes empty, the router sends a prune message upstream to stop delivery of multicast traffic (see [Figure 16 on page 95](#)).

Figure 16: Prune Messages Sent Back to the Source to Stop Unwanted Multicast Traffic



Configuring PIM Dense Mode Properties

In PIM dense mode (PIM-DM), the assumption is that almost all possible subnets have at least one receiver wanting to receive the multicast traffic from a source, so the network is flooded with traffic on all possible branches, then pruned back when branches do not express an interest in receiving the packets, explicitly (by message) or implicitly (time-out silence). LANs are appropriate networks for dense-mode operation.

By default, PIM is disabled. When you enable PIM, it operates in sparse mode by default.

You can configure PIM dense mode globally or for a routing instance. This example shows how to configure the routing instance and how to specify that PIM dense mode use **inet.2** as its RPF routing table instead of **inet.0**.

To configure the router properties for PIM dense mode:

1. (Optional) Create an IPv4 routing table group so that interface routes are installed into two routing tables, **inet.0** and **inet.2**.

```
[edit routing-options rib-groups]
user@host# set pim-rg export-rib inet.0
user@host# set pim-rg import-rib [ inet.0 inet.2 ]
```

2. (Optional) Associate the routing table group with a PIM routing instance.

```
[edit routing-instances PIM.dense protocols pim]
user@host# set rib-group inet pim-rg
```

3. Configure the PIM interface. If you do not specify any interfaces, PIM is enabled on all router interfaces. Generally, you specify interface names only if you are disabling PIM on certain interfaces.

```
[edit routing-instances PIM.dense protocols pim]  
user@host# set interface fe-0/0/1.0 mode dense
```



NOTE: You cannot configure both PIM and Distance Vector Multicast Routing Protocol (DVMRP) in forwarding mode on the same interface. You can configure PIM on the same interface only if you configured DVMRP in unicast-routing mode.

4. Monitor the operation of PIM dense mode by running the **show pim interfaces**, **show pim join**, **show pim neighbors**, and **show pim statistics** commands.

**Related
Documentation**

- [Configuring PIM Sparse-Dense Mode on page 96](#)
- [Configuring Basic PIM Settings on page 77](#)

Configuring PIM Sparse-Dense Mode

- [Understanding PIM Sparse-Dense Mode on page 96](#)
- [Mixing PIM Sparse and Dense Modes on page 96](#)
- [Configuring PIM Sparse-Dense Mode Properties on page 97](#)

Understanding PIM Sparse-Dense Mode

Sparse-dense mode, as the name implies, 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 an RP. Instead, data packets destined for that group are forwarded by means of PIM dense-mode rules. A group specified as sparse is mapped to an RP, and data packets are forwarded by means of PIM sparse-mode rules.

For information about PIM sparse-mode and PIM dense-mode rules, see *Understanding PIM Sparse Mode* and “[Understanding PIM Dense Mode](#)” on page 93.

Mixing PIM Sparse and Dense Modes

It is possible to mix PIM dense mode, PIM sparse mode, and PIM source-specific multicast (SSM) on the same network, the same router, and even the same interface. This is because modes are effectively tied to multicast groups, an IP multicast group address must be unique for a particular group's traffic, and scoping limits enforce the division between potential or actual overlaps.



NOTE: PIM sparse mode was capable of forming shortest-path trees (SPTs) already. Changes to PIM sparse mode to support PIM SSM mainly involved defining behavior in the SSM address range, because shared-tree behavior is prohibited for groups in the SSM address range.

A multicast router employing sparse-dense mode is a good example of mixing PIM modes on the same network or router or interface. Dense modes are easy to support because of the flooding, but scaling issues make dense modes inappropriate for Internet use beyond very restricted uses.

Configuring PIM Sparse-Dense Mode Properties

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 an RP. Instead, data packets destined for that group are forwarded by means of PIM dense mode rules. A group specified as “sparse” is mapped to an RP, and data packets are forwarded by means of PIM sparse-mode rules. Sparse-dense mode is useful in networks implementing auto-RP for PIM sparse mode.

By default, PIM is disabled. When you enable PIM, it operates in sparse mode by default.

You can configure PIM sparse-dense mode globally or for a routing instance. This example shows how to configure PIM sparse-dense mode globally on all interfaces, specifying that the groups 224.0.1.39 and 224.0.1.40 are using dense mode.

To configure the router properties for PIM sparse-dense mode:

1. Configure the dense-mode groups.

```
[protocols pim]  
user@host# set dense-groups 224.0.1.39  
user@host# set dense-groups 224.0.1.40
```

2. Configure all interfaces on the routing device to use sparse-dense mode. When configuring all interfaces, exclude the **fxp0.0** management interface by adding the **disable** statement for that interface.

```
[edit protocols pim]  
user@host# set interface all mode sparse-dense  
user@host# set interface fxp0.0 disable
```

3. Monitor the operation of PIM sparse-dense mode by running the **show pim interfaces**, **show pim join**, **show pim neighbors**, and **show pim statistics** commands.

Related Documentation

- [Configuring PIM Dense Mode on page 93](#)
- [Configuring Basic PIM Settings on page 77](#)

CHAPTER 7

Routing Content to Larger, Sparser Groups with PIM Sparse Mode

- [Configuring PIM Auto-RP on page 99](#)
- [Configuring Embedded RP on page 103](#)
- [Configuring Static RP on page 106](#)
- [Configuring PIM Bootstrap Router on page 113](#)
- [Configuring PIM Filtering on page 117](#)

Configuring PIM Auto-RP

- [Understanding PIM Auto-RP on page 99](#)
- [Configuring PIM Auto-RP on page 99](#)

Understanding PIM Auto-RP

You can configure a more dynamic way of assigning rendezvous points (RPs) in a multicast network by means of auto-RP. When you configure auto-RP for a router, the router learns the address of the RP in the network automatically and has the added advantage of operating in PIM version 1 and version 2.

Although auto-RP is a nonstandard (non-RFC-based) function that typically uses dense mode PIM to advertise control traffic, it provides an important failover advantage that simple static RP assignment does not. You can configure multiple routers as RP candidates. If the elected RP fails, one of the other preconfigured routers takes over the RP functions. This capability is controlled by the auto-RP mapping agent.

Configuring PIM Auto-RP

For correct operation, every multicast router within a PIM domain must be able to map a particular multicast group address to the same rendezvous point (RP). The auto-RP mechanism is one way that a multicast router can learn the set of group-to-RP mappings. Auto-RP automatically distributes mapping information to routing devices. It simplifies use of multiple RPs for different multicast group ranges, thus allowing multiple RPs to act as backups for each other. Auto-RP relies on a router to act as the RP mapping agent. Potential RPs announce themselves to the mapping agent, and the mapping agent resolves any conflicts.

The mapping agent sends the multicast group-RP mapping information to the other routers using PIM dense mode. The specific groups used are 224.0.1.39 and .40. The first (.39) is used to advertise, the second (.40) is used for discovery. Because PIM dense mode is necessary to enable auto-RP to work, which in turn enables PIM sparse mode to work, you must configure PIM sparse-dense mode in the PIM domains that use auto-RP.

Although auto-RP is a nonstandard (non-RFC-based) function requiring dense mode PIM to advertise control traffic, it provides an important failover advantage that static RP assignment does not. That is, you can configure multiple routing devices as RP candidates. If the elected RP fails, one of the other preconfigured routing devices takes over the RP functions. This capability is controlled by the auto-RP mapping agent.

Auto-RP operates in PIM version 1 and version 2.

In most cases, how the routing device handles auto-RP discovery, announce, or mapping messages depends on whether the routing device is an RP (configured as local RP) or not. [Table 6 on page 100](#) shows how the routing device behaves depending on the local RP configuration.

Table 6: Local RP and Auto-RP Message Types

Auto-RP Message Type	Local RP?	Routing Device Behavior
discovery	No	Listen for auto-RP mapping messages.
discovery	Yes	Listen for auto-RP mapping messages.
announce	No	Listen for auto-RP mapping messages.
announce	Yes	Listen for auto-RP mapping messages. Send auto-RP announce messages.
mapping	No	Listen for auto-RP mapping messages. Listen for auto-RP announce messages. If elected mapping agent, send auto-RP mapping messages.
mapping	Yes	Listen for auto-RP mapping messages. Send auto-RP announce messages. Listen for auto-RP announce messages. If elected mapping agent, send auto-RP mapping messages.



NOTE: If the routing device receives auto-RP announcements split across multiple messages, the routing device loses the information in the previous part of the message as soon as the next part of the message is received.

You can configure auto-RP properties globally or for a routing instance. This example shows the global configuration.

To configure auto-RP properties:

1. Configure PIM in sparse-dense mode on all routing devices in the PIM domain.

```
[edit protocols pim]
user@host# edit
user@host# set interface all mode sparse-dense
```

This configuration allows the routing device to operate in sparse mode for most groups and dense mode for others. The default is to operate in sparse mode unless the routing device is specifically informed of a dense mode group.

2. Configure a routable loopback interface address on all routing devices in the PIM domain.

The routing device joins the auto-RP groups on the configured interfaces and on the loopback interface **lo0.0**. For auto-RP to work correctly, configure a routable IP address on the loopback interface. The router ID is used as the address for auto-RP updates. You cannot use the loopback address 127.0.0.1. Also, you must enable PIM sparse-dense mode on the **lo0.0** interface if you do not specify **interface all**.

```
[edit interfaces lo0.0 unit 0 family inet]
user@host# set address 192.168.0.3 preferred
```

3. Configure the two multicast dense groups on all the routing devices.

Auto-RP requires multicast flooding to announce potential RP candidates and to discover the elected RPs in the network. Multicast flooding occurs through a PIM dense mode model, where group 224.0.1.39 is used for **announce** messages and group 224.0.1.40 is used for **discovery** messages.

```
[edit protocols pim]
user@host# set dense-groups 224.0.1.39/32
user@host# set dense-groups 224.0.1.40/32
```



TIP: Step 3 is required. When auto-RP is enabled, the auto-RP announce group (224.0.1.39) and auto-RP-discovery group (224.0.1.40) must be configured explicitly as dense groups. When the auto-RP discovery group is not configured as a dense group, auto-RP is not enabled. When the auto-RP announce group is not configured as a dense group, auto-RP is enabled in the discovery mode only, and mapping and announce modes are disabled.

4. Configure the auto-RP **announce** option.

At least one routing device in the PIM domain must announce auto-RP messages and at least one must map them, or you can configure a routing device to perform both functions.

When a routing device sends announce messages in the network, it is advertising itself as a candidate RP. A routing device configured with this option must also be configured as an RP, or announce messages are not sent.

```
[edit protocols pim rp]
user@host# set local address 192.168.0.1
user@host# set auto-rp announce
```



NOTE: You cannot include the `auto-rp announce` option at the `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim]` hierarchy level.

5. Configure the auto-RP mapping agent.

The mapping agent sends discovery messages to the network, informing all routing devices in a multicast group of which RP to use. If the mapping agent is also an RP, the **mapping** option also allows the routing device to send auto-RP announcements (mapping on an RP allows the routing device to perform both the announcement and mapping functions).

```
[edit protocols pim rp]
user@host# set auto-rp mapping
```

If the mapping agent is also an RP, configure the mapping agent as a local RP.

```
[edit protocols pim rp]
user@host# set local address 192.168.0.2
```

6. Configure mapping agent election.

If you configure the **mapping** option on more than one routing device in the PIM domain, configure mapping agent election on each potential mapping agent.

Auto-RP specifications state that mapping agents do not send mapping messages if they receive messages from a mapping agent with a higher IP address. However, some vendors' mapping agents continue to announce mappings, even in the presence of higher-addressed mapping agents. In other words, some mapping agents will always send mapping messages.

The default auto-RP operation is to perform mapping agent election. To explicitly configure mapping agent election, you can include the **mapping-agent-election** statement. When this option is configured, the mapping agent will stop sending mapping messages if it receives messages from a mapping agent with a higher IP address.

```
[edit protocols pim rp]
user@host# set auto-rp mapping mapping-agent-election
```

Mapping message suppression is disabled with the **no-mapping-agent-election** statement. When this option is configured, the mapping agent will always send mapping messages even in the presence of higher-addressed mapping agents.

To disable mapping agent election for compatibility with other vendors' equipment, include the **no-mapping-agent-election** statement.

```
[edit protocols pim rp]
```



```
user@host# set auto-rp mapping no-mapping-agent-election
```

7. Configure the remaining routing devices in the PIM domain to discover the RP.

Discovery enables the routing devices to receive and process discovery messages from the mapping agent. This is the most basic auto-RP option.

```
[edit protocols pim rp]
user@host# set auto-rp discovery
```

8. Monitor the operation of PIM auto-RP routers by running the following commands:

- `show pim interfaces`
- `show pim rps`
- `show pim rps`

9. Issue the `show pim rps extensive` command to see information about how an RP is learned, what groups it handles, and the number of groups actively using the RP.

```
user@host> show pim rps extensive
RP: 192.168.5.1
Learned from 192.168.5.1 via: auto-rp
Time Active: 00:34:29
Holdtime: 150 with 108 remaining
Device Index: 6
Subunit: 32769
Interface: pd-0/0/0.32769
Group Ranges:
    224.0.0.0/4
Active groups using RP:
    224.2.2.100
    total 1 groups active
Register State for RP:
Group      Source FirstHop      RP Address      StateRP address Type Holdtime
Timeout
```

In the example, the RP at 192.168.5.1 was learned through auto-RP. The RP is able to support all groups in the 224.0.0.0/4 range (all possible groups). The local router has sent PIM control traffic for the 224.2.2.100 group to the RP.

Additionally, the presence of a Tunnel Physical Interface Card (PIC) in an RP router creates a de-encapsulation interface, which allows the RP to receive multicast traffic from the source. This interface is indicated by `pd-0/0/0.32769`.

Related Documentation

- [Configuring PIM Bootstrap Router on page 113](#)
- [Configuring a Designated Router for PIM on page 90](#)
- *Examples: Configuring PIM Sparse Mode*
- [Configuring Basic PIM Settings on page 77](#)

Configuring Embedded RP

- [Understanding Embedded RP for IPv6 Multicast on page 104](#)
- [Configuring PIM Embedded RP for IPv6 on page 105](#)

Understanding Embedded RP for IPv6 Multicast

Global IPv6 multicast between routing domains has been possible only with source-specific multicast (SSM) because there is no way to convey information about IPv6 multicast RPs between PIM sparse mode RPs. In IPv4 multicast networks, this information is conveyed between PIM RPs using MSDP, but there is no IPv6 support in current MSDP standards. IPv6 uses the concept of an embedded RP to resolve this issue without requiring SSM. This feature embeds the RP address in an IPv6 multicast address.

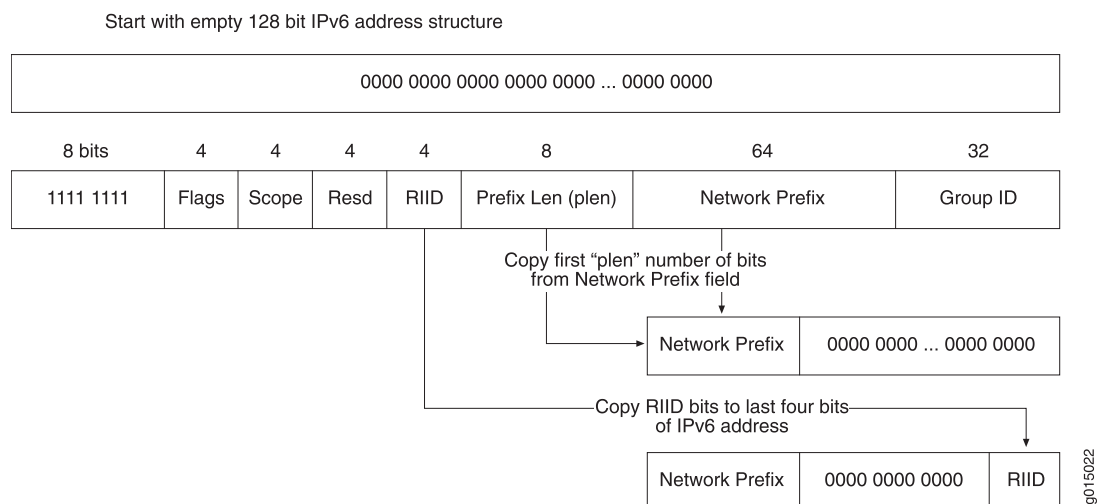
All IPv6 multicast addresses begin with 8 1-bits (1111 1111) followed by a 4-bit flag field normally set to 0011. The flag field is set to 0111 when embedded RP is used. Then the low-order bits of the normally reserved field in the IPv6 multicast address carry the 4-bit RP interface identifier (RIID).

When the IPv6 address of the RP is embedded in a unicast-prefix-based any-source multicast (ASM) address, all of the following conditions must be true:

- The address must be an IPv6 multicast address and have 0111 in the flags field (that is, the address is part of the prefix FF70::/12).
- The 8-bit prefix length (plen) field must not be all 0. An all 0 plen field implies that SSM is in use.
- The 8-bit prefix length field value must not be greater than 64, which is the length of the network prefix field in unicast-prefix-based ASM addresses.

The routing platform derives the value of the interdomain RP by copying the prefix length field number of bits from the 64-bit network prefix field in the received IPv6 multicast address to an empty 128-bit IPv6 address structure and copying the last bits from the 4-bit RIID. For example, if the prefix length field bits have the value 32, then the routing platform copies the first 32 bits of the IPv6 multicast address network prefix field to an all-0 IPv6 address and appends the last four bits determined by the RIID. See [Figure 17 on page 104](#) for an illustration of this process.

Figure 17: Extracting the Embedded RP IPv6 Address



For example, the administrator of IPv6 network 2001:DB8::/32 sets up an RP for the 2001:DB8:BEEF:FEED::/96 subnet. In that case, the received embedded RP IPv6 ASM address has the form:

`FF70:y40:2001:DB8:BEEF:FEED::/96`

and the derived RP IPv6 address has the form:

`2001:DB8:BEEF:FEED::y`

where *y* is the RIID (*y* cannot be 0).

When configured, the routing platform checks for embedded RP information in every PIM join request received for IPv6. The use of embedded RP does not change the processing of IPv6 multicast and RPs in any way, except that the embedded RP address is used if available and selected for use. There is no need to specify the IPv6 address family for embedded RP configuration because the information can be used only if IPv6 multicast is properly configured on the routing platform.

The following receive events trigger extraction of an IPv6 embedded RP address on the routing platform:

- 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

The embedded RP node discovered through these events is added if it does not already exist on the routing platform. The routing platform chooses the embedded RP as the RP for a multicast group before choosing an RP learned through BSRs or a statically configured RP. 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.

Configuring PIM Embedded RP for IPv6

You configure embedded RP to allow multidomain IPv6 multicast networks to find RPs in other routing domains. Embedded RP embeds an RP address inside PIM join messages and other types of messages sent between routing domains. Global IPv6 multicast between routing domains has been possible only with source-specific multicast (SSM) because there is no way to convey information about IPv6 multicast RPs between PIM sparse mode RPs. In IPv4 multicast networks, this information is conveyed between PIM RPs using MSDP, but there is no IPv6 support in current MSDP standards. IPv6 uses the concept of an embedded RP to resolve this issue without requiring SSM. Thus, embedded RP enables you can deploy IPv6 with any-source multicast (ASM).

Embedded RP is disabled by default.

When you configure embedded RP for IPv6, embedded RPs are preferred to RPs discovered by IPv6 any other way. You configure embedded RP independent of any other IPv6 multicast properties. This feature is applied only when IPv6 multicast is properly configured.

You can configure embedded RP globally or for a routing instance. This example shows the routing instance configuration.

To configure embedded RP for IPv6 PIM sparse mode:

1. Define which multicast addresses or prefixes can embed RP address information. If messages within a group range contain embedded RP information and the group range is not configured, the embedded RP in that group range is ignored. Any valid unicast-prefix-based ASM address can be used as a group range. The default group range is FF70::/12 to FFF0::/12. Messages with embedded RP information that do not match any configured group ranges are treated as normal multicast addresses.

```
[edit routing-instances vpn-A protocols pim rp embedded-rp]
user@host# set group-ranges fec0::/10
```

If the derived RP address is not a valid IPv6 unicast address, it is treated as any other multicast group address and is not used for RP information. Verification fails if the extracted RP address is a local interface, unless the routing device is configured as an RP and the extracted RP address matches the configured RP address. Then the local RP determines whether it is configured to act as an RP for the embedded RP multicast address.

2. Limit the number of embedded RPs created in a specific routing instance. The range is from 1 through 500. The default is 100.

```
[edit routing-instances vpn-A protocols pim rp]
user@host# set maximum-rps 50
```

3. Monitor the operation by running the **show pim rps** and **show pim statistics** commands.

Related Documentation

- [Configuring PIM Auto-RP on page 99](#)
- [Configuring PIM Bootstrap Router on page 113](#)
- [Configuring a Designated Router for PIM on page 90](#)
- [Examples: Configuring PIM Sparse Mode](#)
- [Configuring Basic PIM Settings on page 77](#)

Configuring Static RP

- [Understanding Static RP on page 106](#)
- [Configuring Local PIM RPs on page 107](#)
- [Example: Configuring PIM Sparse Mode and RP Static IP Addresses on page 109](#)
- [Configuring the Static PIM RP Address on the Non-RP Routing Device on page 111](#)

Understanding Static RP

Protocol Independent Multicast (PIM) sparse mode is the most common multicast protocol used on the Internet. PIM sparse mode is the default mode whenever PIM is configured on any interface of the device. However, because PIM must not be configured on the network management interface, you must disable it on that interface.

Each any-source multicast (ASM) group has a shared tree through which receivers learn about new multicast sources and new receivers learn about all multicast sources. The rendezvous point (RP) router is the root of this shared tree and receives the multicast traffic from the source. To receive multicast traffic from the groups served by the RP, the device must determine the IP address of the RP for the source.

You can configure a static rendezvous point (RP) configuration that is similar to static routes. A static configuration has the benefit of operating in PIM version 1 or version 2. When you configure the static RP, the RP address that you select for a particular group must be consistent across all routers in a multicast domain.

One common way for the device to locate RPs is by static configuration of the IP address of the RP. A static configuration is simple and convenient. However, if the statically defined RP router becomes unreachable, there is no automatic failover to another RP router. To remedy this problem, you can use anycast RP.

Configuring Local PIM RPs

Local RP configuration makes the routing device a statically defined RP. Consider statically defining an RP if the network does not have many different RPs defined or if the RP assignment does not change very often. The Junos IPv6 PIM implementation supports only static RP configuration. Automatic RP announcement and bootstrap routers are not available with IPv6.

You can configure a local RP globally or for a routing instance. This example shows how to configure a local RP in a routing instance for IPv4 or IPv6.

To configure the routing device's RP properties:

1. Configure the routing instance as the local RP.

```
[routing-instances VPN-A protocols pim]
user@host# set rp local
```

2. Configure the IP protocol family and IP address.

IPv6 PIM hello messages are sent to every interface on which you configure **family inet6**, whether at the PIM level of the hierarchy or not. As a result, if you configure an interface with both **family inet** at the **[edit interface interface-name]** hierarchy level and **family inet6** at the **[edit protocols pim interface interface-name]** hierarchy level, PIM sends both IPv4 and IPv6 hellos to that interface.

By default, PIM operates in sparse mode on an interface. If you explicitly configure sparse mode, PIM uses this setting for all IPv6 multicast groups. However, if you configure sparse-dense mode, PIM does not accept IPv6 multicast groups as dense groups and operates in sparse mode over them.

```
[edit routing-instances VPN-A protocols pim rp local]
user@host# set family inet6 address 2001:db8:85a3::8a2e:370:7334
user@host# set family inet address 10.1.2.254
```

3. (IPv4 only) Configure the routing device's RP priority.



NOTE: The priority statement is not supported for IPv6, but is included here for informational purposes. The routing device's priority value for becoming the RP is included in the bootstrap messages that the routing device sends. Use a smaller number to increase the likelihood that the routing device becomes the RP for local multicast groups. Each PIM routing device uses the priority value and other factors to determine the candidate RPs for a particular group range. After the set of candidate RPs is distributed, each routing device determines algorithmically the RP from the candidate RP set using a hash function. By default, the priority value is set to 1. If this value is set to 0, the bootstrap router can override the group range being advertised by the candidate RP.

```
[edit routing-instances VPN-A protocols pim rp local]
user@host# set priority 5
```

4. Configure the groups for which the routing device is the RP.

By default, a routing device running PIM is eligible to be the RP for all IPv4 or IPv6 groups (224.0.0.0/4 or FF70::/12 to FFF0::/12). The following example limits the groups for which this routing device can be the RP.

```
[edit routing-instances VPN-A protocols pim rp local]
user@host# set group-ranges fec0::/10
user@host# set group-ranges 10.1.2.0/24
```

5. (IPv4 only) Modify the local RP hold time.

If the local routing device is configured as an RP, it is considered a candidate RP for its local multicast groups. For candidate RPs, the hold time is used by the bootstrap router to time out RPs, and applies to the bootstrap RP-set mechanism. The RP hold time is part of the candidate RP advertisement message sent by the local routing device to the bootstrap router. If the bootstrap router does not receive a candidate RP advertisement from an RP within the hold time, it removes that routing device from its list of candidate RPs. The default hold time is 150 seconds.

```
[edit routing-instances VPN-A protocols pim rp local]
user@host# set hold-time 200
```

6. (Optional) Override dynamic RP for the specified group address range.

If you configure both static RP mapping and dynamic RP mapping (such as auto-RP) in a single routing instance, allow the static mapping to take precedence for the given static RP group range, and allow dynamic RP mapping for all other groups.

If you exclude this statement from the configuration and you use both static and dynamic RP mechanisms for different group ranges within the same routing instance, the dynamic RP mapping takes precedence over the static RP mapping, even if static RP is defined for a specific group range.

```
[edit routing-instances VPN-A protocols pim rp local]
user@host# set override
```

7. Monitor the operation of PIM by running the **show pim** commands. Run **show pim ?** to display the supported commands.

Example: Configuring PIM Sparse Mode and RP Static IP Addresses

This example shows how to configure PIM sparse mode and RP static IP addresses.

- [Requirements on page 109](#)
- [Overview on page 109](#)
- [Configuration on page 109](#)
- [Verification on page 111](#)

Requirements

Before you begin:

1. Determine whether the router is directly attached to any multicast sources. Receivers must be able to locate these sources.
2. Determine whether the router is directly attached to any multicast group receivers. If receivers are present, IGMP is needed.
3. Determine whether to configure multicast to use sparse, dense, or sparse-dense mode. Each mode has different configuration considerations.
4. Determine the address of the RP if sparse or sparse-dense mode is used.
5. Determine whether to locate the RP with the static configuration, BSR, or auto-RP method.
6. Determine whether to configure multicast to use its own RPF routing table when configuring PIM in sparse, dense, or sparse-dense mode.
7. Configure the SAP and SDP protocols to listen for multicast session announcements.
8. Configure IGMP.

Overview

In this example, you set the interface value to **all** and disable the **ge-0/0/0** interface. Then you configure the IP address of the RP as **192.168.14.27**.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set protocols pim interface all
set protocols pim interface ge-0/0/0 disable
set protocols pim rp static address 192.168.14.27
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure PIM sparse mode and the RP static IP address:

1. Configure PIM.

```
[edit]  
user@host# edit protocols pim
```
2. Set the interface value.

```
[edit protocols pim]  
user@host# set pim interface all
```
3. Disable PIM on the network management interface.

```
[edit protocols pim interface]  
user@host# set pim interface ge-0/0/0 unit 0 disable
```
4. Configure RP.

```
[edit]  
user@host# edit protocols pim rp
```
5. Configure the IP address of the RP.

```
[edit]  
user@host# set static address 192.168.14.27
```

Results From configuration mode, confirm your configuration by entering the **show protocols** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]  
user@host# show protocols  
pim {  
  rp {  
    static {  
      address 192.168.14.27;  
    }  
  }  
}  
interface all;  
  interface ge-0/0/0.0 {  
    disable;  
  }  
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying SAP and SDP Addresses and Ports on page 111](#)
- [Verifying the IGMP Version on page 111](#)
- [Verifying the PIM Mode and Interface Configuration on page 111](#)

Verifying SAP and SDP Addresses and Ports

Purpose Verify that SAP and SDP are configured to listen on the correct group addresses and ports.

Action From operational mode, enter the **show sap listen** command.

Verifying the IGMP Version

Purpose Verify that IGMP version 2 is configured on all applicable interfaces.

Action From operational mode, enter the **show igmp interface** command.

Verifying the PIM Mode and Interface Configuration

Purpose Verify that PIM sparse mode is configured on all applicable interfaces.

Action From operational mode, enter the **show pim interfaces** command.

Configuring the Static PIM RP Address on the Non-RP Routing Device

Consider statically defining an RP if the network does not have many different RPs defined or if the RP assignment does not change very often. The Junos IPv6 PIM implementation supports only static RP configuration. Automatic RP announcement and bootstrap routers are not available with IPv6.

You configure a static RP address on the non-RP routing device. This enables the non-RP routing device to recognize the local statically defined RP. For example, if R0 is a non-RP router and R1 is the local RP router, you configure R0 with the static RP address of R1. The static IP address is the routable address assigned to the loopback interface on R1. In the following example, the loopback address of the RP is 2001:db8:85a3::8a2e:370:7334.

You can configure a static RP address globally or for a routing instance. This example shows how to configure a static RP address in a routing instance for IPv6.

To configure the static RP address:

1. On a non-RP routing device, configure the routing instance to point to the routable address assigned to the loopback interface of the RP.

```
[routing-instances VPN-A protocols pim rp]
user@host# set static address 2001:db8:85a3::8a2e:370:7334
```



NOTE: Logical systems are also supported. You can configure a static RP address in a logical system only if the logical system is not directly connected to a source.

2. (Optional) Set the PIM sparse mode version.

For each static RP address, you can optionally specify the PIM version. The default PIM version is version 1.

```
[edit routing-instances VPN-A protocols pim rp]
user@host# set static address 2001:db8:85a3::8a2e:370:7334 version 2
```



NOTE: The default PIM version can be version 1 or version 2, depending on the mode you are configuring. PIM version 1 is the default for RP mode ([edit pim rp static address *address*]). PIM version 2 is the default for interface mode ([edit pim interface *interface-name*]). Explicitly configured versions override the defaults.

3. (Optional) Set the group address range.

By default, a routing device running PIM is eligible to be the RP for all IPv4 or IPv6 groups (224.0.0.0/4 or FF70::/12 to FFF0::/12). The following example limits the groups for which the 2001:db8:85a3::8a2e:370:7334 address can be the RP.

```
[edit routing-instances VPN-A protocols pim rp]
user@host# set static address 2001:db8:85a3::8a2e:370:7334 group-ranges fec0::/10
```

The RP that you select for a particular group must be consistent across all routers in a multicast domain.

4. (Optional) Override dynamic RP for the specified group address range.

If you configure both static RP mapping and dynamic RP mapping (such as auto-RP) in a single routing instance, allow the static mapping to take precedence for the given static RP group range, and allow dynamic RP mapping for all other groups.

If you exclude this statement from the configuration and you use both static and dynamic RP mechanisms for different group ranges within the same routing instance, the dynamic RP mapping takes precedence over the static RP mapping, even if static RP is defined for a specific group range.

```
[edit routing-instances VPN-A protocols pim rp static address
 2001:db8:85a3::8a2e:370:7334]
user@host# set override
```

5. Monitor the operation of PIM by running the **show pim** commands. Run **show pim ?** to display the supported commands.

Related Documentation

- [Configuring PIM Auto-RP on page 99](#)
- [Configuring PIM Bootstrap Router on page 113](#)
- [Configuring a Designated Router for PIM on page 90](#)

- [Examples: Configuring PIM Sparse Mode](#)
- [Configuring Basic PIM Settings on page 77](#)

Configuring PIM Bootstrap Router

- [Understanding the PIM Bootstrap Router on page 113](#)
- [Configuring PIM Bootstrap Properties for IPv4 on page 113](#)
- [Configuring PIM Bootstrap Properties for IPv4 or IPv6 on page 114](#)
- [Example: Rejecting PIM Bootstrap Messages at the Boundary of a PIM Domain on page 116](#)
- [Example: Configuring PIM BSR Filters on page 117](#)

Understanding the PIM Bootstrap Router

To determine which router is the rendezvous point (RP), all routers within a PIM sparse-mode domain collect bootstrap messages. A PIM sparse-mode domain is a group of routers that all share the same RP router. The domain bootstrap router initiates bootstrap messages, which are sent hop by hop within the domain. The routers use bootstrap messages to distribute RP information dynamically and to elect a bootstrap router when necessary.

Configuring PIM Bootstrap Properties for IPv4

For correct operation, every multicast router within a PIM domain must be able to map a particular multicast group address to the same Rendezvous Point (RP). The bootstrap router mechanism is one way that a multicast router can learn the set of group-to-RP mappings. Bootstrap routers are supported in IPv4 and IPv6.



NOTE: For legacy configuration purposes, there are two sections that describe the configuration of bootstrap routers: one section for both IPv4 and IPv6, and this section, which is for IPv4 only. The method described in [“Configuring PIM Bootstrap Properties for IPv4 or IPv6” on page 114](#) is recommended. A commit error occurs if the same IPv4 bootstrap statements are included in both the IPv4-only and the IPv4-and-IPv6 sections of the hierarchy. The error message is “duplicate IPv4 bootstrap configuration.”

To determine which routing device is the RP, all routing devices within a PIM domain collect bootstrap messages. A PIM domain is a contiguous set of routing devices that implement PIM. All are configured to operate within a common boundary. The domain's bootstrap router initiates bootstrap messages, which are sent hop by hop within the domain. The routing devices use bootstrap messages to distribute RP information dynamically and to elect a bootstrap router when necessary.

PIM bootstrap messages are sourced from the loopback address, which is always up. The loopback address must be routable; if it is not routable, then the bootstrap router is

unable to send bootstrap messages to update the RP domain members. See *Configuring the Loopback Interface* for information about configuring a loopback interface.

You can configure bootstrap properties globally or for a routing instance. This example shows the global configuration.

To configure the bootstrap router properties:

1. Configure the bootstrap priority.

By default, each routing device has a bootstrap priority of 0, which means the routing device can never be the bootstrap router. A priority of 0 disables the function for IPv4 and does not cause the routing device to send bootstrap router packets with a 0 in the priority field. The routing device with the highest priority value is elected to be the bootstrap router. In the case of a tie, the routing device with the highest IP address is elected to be the bootstrap router. A simple bootstrap configuration assigns a bootstrap priority value to a routing device.

```
[edit protocols pim rp]
user@host# set bootstrap-priority 3
```

2. (Optional) Create import and export policies to control the flow of IPv4 bootstrap messages to and from the RP, and apply the policies to PIM. Import and export policies are useful when some of the routers in your PIM domain have interfaces that connect to other PIM domains. Configuring a policy prevents bootstrap messages from crossing domain boundaries. The **bootstrap-import** statement prevents messages from being imported into the RP. The **bootstrap-export** statement prevents messages from being exported from the RP.

```
[edit protocols pim rp]
user@host# set bootstrap-import pim-bootstrap-import
user@host# set bootstrap-export pim-bootstrap-export
```

3. Configure the policies.

```
[edit policy-options policy-statement pim-bootstrap-import]
user@host# set from interface se-0/0/0
user@host# set then reject
```

```
[edit policy-options policy-statement pim-bootstrap-export]
user@host# set from interface se-0/0/0
user@host# set then reject
```

4. Monitor the operation of PIM bootstrap routers by running the **show pim bootstrap** command.

Configuring PIM Bootstrap Properties for IPv4 or IPv6

For correct operation, every multicast router within a PIM domain must be able to map a particular multicast group address to the same Rendezvous Point (RP). The bootstrap router mechanism is one way that a multicast router can learn the set of group-to-RP mappings. Bootstrap routers are supported in IPv4 and IPv6.



NOTE: For legacy configuration purposes, there are two sections that describe the configuration of bootstrap routers: one section for IPv4 only, and this section, which is for both IPv4 and IPv6. The method described in this section is recommended. A commit error occurs if the same IPv4 bootstrap statements are included in both the IPv4-only and the IPv4-and-IPv6 sections of the hierarchy. The error message is “duplicate IPv4 bootstrap configuration.”

To determine which routing device is the RP, all routing devices within a PIM domain collect bootstrap messages. A PIM domain is a contiguous set of routing devices that implement PIM. All devices are configured to operate within a common boundary. The domain's bootstrap router initiates bootstrap messages, which are sent hop by hop within the domain. The routing devices use bootstrap messages to distribute RP information dynamically and to elect a bootstrap router when necessary.

PIM bootstrap messages are sourced from the loopback address, which is always up. The loopback address must be routable; if it is not routable, then the bootstrap router is unable to send bootstrap messages to update the RP domain members. See *Configuring the Loopback Interface* for information about configuring a loopback interface.

You can configure bootstrap properties globally or for a routing instance. This example shows the global configuration.

To configure the bootstrap router properties:

1. Configure the bootstrap priority.

By default, each routing device has a bootstrap priority of 0, which means the routing device can never be the bootstrap router. The routing device with the highest priority value is elected to be the bootstrap router. In the case of a tie, the routing device with the highest IP address is elected to be the bootstrap router. A simple bootstrap configuration assigns a bootstrap priority value to a routing device.



NOTE: In the IPv4-only configuration, specifying a bootstrap priority of 0 disables the bootstrap function and does not cause the routing device to send BSR packets with a 0 in the priority field. In the configuration shown here, specifying a bootstrap priority of 0 does not disable the function, but causes the routing device to send BSR packets with a 0 in the priority field. To disable the bootstrap function in the IPv4 and IPv6 configuration, delete the `bootstrap` statement.

```
user@host# edit protocols pim rp
user@host# set bootstrap family inet priority 3
```

2. (Optional) Create import and export policies to control the flow of bootstrap messages to and from the RP, and apply the policies to PIM. Import and export policies are useful when some of the routers in your PIM domain have interfaces that connect to other PIM domains. Configuring a policy prevents bootstrap messages from crossing domain

boundaries. The **import** statement prevents messages from being imported into the RP. The **export** statement prevents messages from being exported from the RP.

```
[edit protocols pim rp]
user@host# set bootstrap family inet import pim-bootstrap-import
user@host# set bootstrap family inet export pim-bootstrap-export
```

3. Configure the policies.

```
[edit policy-options policy-statement pim-bootstrap-import]
user@host# set from interface se-0/0/0
user@host# set then reject
user@host# exit
user@host# edit policy-options policy-statement pim-bootstrap-export
user@host# set from interface se-0/0/0
user@host# set then reject
```

4. Monitor the operation of PIM bootstrap routers by running the **show pim bootstrap** command.

Example: Rejecting PIM Bootstrap Messages at the Boundary of a PIM Domain

In this example, the **from interface so-0-1/0 then reject** policy statement rejects bootstrap messages from the specified interface (the example is configured for both IPv4 and IPv6 operation):

```
protocols {
  pim {
    rp {
      bootstrap {
        family inet {
          priority 1;
          import pim-import;
          export pim-export;
        }
        family inet6 {
          priority 1;
          import pim-import;
          export pim-export;
        }
      }
    }
  }
}
policy-options {
  policy-statement pim-import {
    from interface so-0/1/0;
    then reject;
  }
  policy-statement pim-export {
    to interface so-0/1/0;
    then reject;
  }
}
```

Example: Configuring PIM BSR Filters

Configure a filter to prevent BSR messages from entering or leaving your network. Add this configuration to all routers:

```
protocols {
  pim {
    rp {
      bootstrap-import no-bsr;
      bootstrap-export no-bsr;
    }
  }
}
policy-options {
  policy-statement no-bsr {
    then reject;
  }
}
```

Related Documentation

- [Configuring PIM Auto-RP on page 99](#)
- [Configuring a Designated Router for PIM on page 90](#)
- *Examples: Configuring PIM Sparse Mode*
- [Configuring Basic PIM Settings on page 77](#)

Configuring PIM Filtering

- [Understanding Multicast Message Filters on page 117](#)
- [Filtering MAC Addresses on page 118](#)
- [Filtering RP and DR Register Messages on page 118](#)
- [Filtering MSDP SA Messages on page 119](#)
- [Configuring Interface-Level PIM Neighbor Policies on page 120](#)
- [Filtering Outgoing PIM Join Messages on page 121](#)
- [Example: Stopping Outgoing PIM Register Messages on a Designated Router on page 122](#)
- [Filtering Incoming PIM Join Messages on page 124](#)
- [Example: Rejecting Incoming PIM Register Messages on RP Routers on page 126](#)
- [Configuring Register Message Filters on a PIM RP and DR on page 128](#)

Understanding Multicast Message Filters

Multicast sources and routers generate a considerable number of control messages, especially when using PIM sparse mode. These messages form distribution trees, locate rendezvous points (RPs) and designated routers (DRs), and transition from one type of tree to another. In most cases, this multicast messaging system operates transparently and efficiently. However, in some configurations, more control over the sending and receiving of multicast control messages is necessary.

You can configure multicast filtering to control the sending and receiving of multicast control messages.

To prevent unauthorized groups and sources from registering with an RP router, you can define a routing policy to reject PIM register messages from specific groups and sources and configure the policy on the designated router or the RP router.

- If you configure the reject policy on an RP router, it rejects incoming PIM register messages from the specified groups and sources. The RP router also sends a register stop message by means of unicast to the designated router. On receiving the register stop message, the designated router sends periodic null register messages for the specified groups and sources to the RP router.
- If you configure the reject policy on a designated router, it stops sending PIM register messages for the specified groups and sources to the RP router.



NOTE: If you have configured the reject policy on an RP router, we recommend that you configure the same policy on all the RP routers in your multicast network.



NOTE: If you delete a group and source address from the reject policy configured on an RP router and commit the configuration, the RP router will register the group and source only when the designated router sends a null register message.

Filtering MAC Addresses

When a router is exclusively configured with multicast protocols on an interface, multicast sets the interface media access control (MAC) filter to multicast promiscuous mode, and the number of multicast groups is unlimited. However, when the router is not exclusively used for multicasting and other protocols such as OSPF, Routing Information Protocol version 2 (RIPv2), or Network Time Protocol (NTP) are configured on an interface, each of these protocols individually requests that the interface program the MAC filter to pick up its respective multicast group only. In this case, without multicast configured on the interface, the maximum number of multicast MAC filters is limited to 20. For example, the maximum number of interface MAC filters for protocols such as OSPF (multicast group 224.0.0.5) is 20, unless a multicast protocol is also configured on the interface.

No configuration is necessary for MAC filters.

Filtering RP and DR Register Messages

You can filter Protocol Independent Multicast (PIM) register messages sent from the designated router (DR) or to the rendezvous point (RP). The PIM RP keeps track of all active sources in a single PIM sparse mode domain. In some cases, more control over which sources an RP discovers, or which sources a DR notifies other RPs about, is desired. A high degree of control over PIM register messages is provided by RP and DR register

message filtering. Message filtering also prevents unauthorized groups and sources from registering with an RP router.

Register messages that are filtered at a DR are not sent to the RP, but the sources are available to local users. Register messages that are filtered at an RP arrive from source DRs, but are ignored by the router. Sources on multicast group traffic can be limited or directed by using RP or DR register message filtering alone or together.

If the action of the register filter policy is to discard the register message, the router needs to send a register-stop message to the DR. Register-stop messages are throttled to prevent malicious users from triggering them on purpose to disrupt the routing process.

Multicast group and source information is encapsulated inside unicast IP packets. This feature allows the router to inspect the multicast group and source information before sending or accepting the PIM register message.

Incoming register messages to an RP are passed through the configured register message filtering policy before any further processing. If the register message is rejected, the RP router sends a register-stop message to the DR. When the DR receives the register-stop message, the DR stops sending register messages for the filtered groups and sources to the RP. Two fields are used for register message filtering:

- Group multicast address
- Source address

The syntax of the existing policy statements is used to configure the filtering on these two fields. The **route-filter** statement is useful for multicast group address filtering, and the **source-address-filter** statement is useful for source address filtering. In most cases, the action is to **reject** the register messages, but more complex filtering policies are possible.

Filtering cannot be performed on other header fields, such as DR address, protocol, or port. In some configurations, an RP might not send register-stop messages when the policy action is to discard the register messages. This has no effect on the operation of the feature, but the router will continue to receive register messages.

When anycast RP is configured, register messages can be sent or received by the RP. All the RPs in the anycast RP set need to be configured with the same RP register message filtering policies. Otherwise, it might be possible to circumvent the filtering policy.

Filtering MSDP SA Messages

Along with applying MSDP source active (SA) filters on all external MSDP sessions (in and out) to prevent SAs for groups and sources from leaking in and out of the network, you need to apply bootstrap router (BSR) filters. Applying a BSR filter to the boundary of a network prevents foreign BSR messages (which announce RP addresses) from leaking into your network. Since the routers in a PIM sparse-mode domain need to know the address of only one RP router, having more than one in the network can create issues.

If you did not use multicast scoping to create boundary filters for all customer-facing interfaces, you might want to use PIM join filters. Multicast scopes prevent the actual

multicast data packets from flowing in or out of an interface. PIM join filters prevent PIM sparse-mode state from being created in the first place. Since PIM join filters apply only to the PIM sparse-mode state, it might be more beneficial to use multicast scoping to filter the actual data.



NOTE: When you apply firewall filters, firewall action modifiers, such as **log**, **sample**, and **count**, work only when you apply the filter on an inbound interface. The modifiers do not work on an outbound interface.

Configuring Interface-Level PIM Neighbor Policies

You can configure a policy to filter unwanted PIM neighbors. In the following example, the PIM interface compares neighbor IP addresses with the IP address in the policy statement before any hello processing takes place. If any of the neighbor IP addresses (primary or secondary) match the IP address specified in the prefix list, PIM drops the hello packet and rejects the neighbor.

If you configure a PIM neighbor policy after PIM has already established a neighbor adjacency to an unwanted PIM neighbor, the adjacency remains intact until the neighbor hold time expires. When the unwanted neighbor sends another hello message to update its adjacency, the router recognizes the unwanted address and rejects the neighbor.

To configure a policy to filter unwanted PIM neighbors:

1. Configure the policy. The neighbor policy must be a properly structured policy statement that uses a prefix list (or a route filter) containing the neighbor primary address (or any secondary IP addresses) in a prefix list, and the **reject** option to reject the unwanted address.

```
[edit policy-options]
user@host# set prefix-list nbrGroup 1 20.20.20.1/32
user@host# set policy-statement nbr-policy from prefix-list nbrGroup1
user@host# set policy-statement nbr-policy then reject
```

2. Configure the interface globally or in the routing instance. This example shows the configuration for the routing instance.

```
[edit routing-instances PIM.master protocols pim]
user@host# set neighbor-policy nbr-policy
```

3. Verify the configuration by checking the **Hello dropped on neighbor policy** field in the output of the **show pim statistics** command.

Filtering Outgoing PIM Join Messages

When the core of your network is using MPLS, PIM join and prune messages stop at the customer edge (CE) routers and are not forwarded toward the core, because these routers do not have PIM neighbors on the core-facing interfaces. When the core of your network is using IP, PIM join and prune messages are forwarded to the upstream PIM neighbors in the core of the network.

When the core of your network is using a mix of IP and MPLS, you might want to filter certain PIM join and prune messages at the upstream egress interface of the CE routers.

You can filter PIM sparse mode (PIM-SM) join and prune messages at the egress interfaces for IPv4 and IPv6 in the upstream direction. The messages can be filtered based on the group address, source address, outgoing interface, PIM neighbor, or a combination of these values. If the filter is removed, the join is sent after the PIM periodic join timer expires.

To filter PIM sparse mode join and prune messages at the egress interfaces, create a policy rejecting the group address, source address, outgoing interface, or PIM neighbor, and then apply the policy.

The following example filters PIM join and prune messages for group addresses 224.0.1.2 and 225.1.1.1.

1. In configuration mode, create the policy.

```
user@host# set policy-options policy-statement block-groups term t1 from route-filter
224.0.1.2/32 exact
user@host# set policy-options policy-statement block-groups term t1 from route-filter
225.1.1.1/32 exact
user@host# set policy-options policy-statement block-groups term t1 then reject
user@host# set policy-options policy-statement block-groups term last then accept
```

2. Verify the policy configuration by running the **show policy-options** command.

```
user@host# show policy-options
policy-statement block-groups {
  term t1 {
    from {
      route-filter 224.0.1.2/32 exact;
      route-filter 225.1.1.1/32 exact;
      then reject;
    }
    term last {
      then accept;
    }
  }
}
```

3. Apply the PIM join and prune message filter.

```
user@host> set protocols pim export block-groups
```

4. After the configuration is committed, use the **show pim statistics** command to verify that outgoing PIM join and prune messages are being filtered.

```
user@host> show pim statistics | grep filtered
```

RP Filtered Source	0
Rx Joins/Prunes filtered	0
Tx Joins/Prunes filtered	254

The egress filter count is shown on the **Tx Joins/Prunes filtered** line.

Example: Stopping Outgoing PIM Register Messages on a Designated Router

This example shows how to stop outgoing PIM register messages on a designated router.

- [Requirements on page 122](#)
- [Overview on page 122](#)
- [Configuration on page 123](#)
- [Verification on page 124](#)

Requirements

Before you begin:

1. Determine whether the router is directly attached to any multicast sources. Receivers must be able to locate these sources.
2. Determine whether the router is directly attached to any multicast group receivers. If receivers are present, IGMP is needed.
3. Determine whether to configure multicast to use sparse, dense, or sparse-dense mode. Each mode has different configuration considerations.
4. Determine the address of the RP if sparse or sparse-dense mode is used.
5. Determine whether to locate the RP with the static configuration, BSR, or auto-RP method.
6. Determine whether to configure multicast to use its own RPF routing table when configuring PIM in sparse, dense, or sparse-dense mode.
7. Configure the SAP and SDP protocols to listen for multicast session announcements.
8. Configure IGMP.
9. Configure the PIM static RP.
10. Filter PIM register messages from unauthorized groups and sources. See [“Example: Rejecting Incoming PIM Register Messages on RP Routers” on page 126](#).

Overview

In this example, you configure the group address as **224.2.2.2/32** and the source address in the group as **20.20.20.1/32**. You set the match action to not send PIM register messages for the group and source address. Then you configure the policy on the designated router to **stop-pim-register-msg-dr**.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set policy-options policy-statement stop-pim-register-msg-dr from route-filter
  224.2.2.2/32 exact
set policy-options policy-statement stop-pim-register-msg-dr from source-address-filter
  20.20.20.1/32 exact
set policy-options policy-statement stop-pim-register-msg-dr then reject
set protocols pim rp dr-register-policy stop-pim-register-msg-dr
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To stop outgoing PIM register messages on a designated router:

1. Configure the policy options.

```
[edit]
user@host# edit policy-options
```

2. Set the group address.

```
[edit policy-options]
user@host# set policy statement stop-pim-register-msg-dr from route-filter
  224.2.2.2/32 exact
```

3. Set the source address.

```
[edit policy-options]
user@host# set policy statement stop-pim-register-msg-dr from
  source-address-filter 20.20.20.1/32 exact
```

4. Set the match action.

```
[edit policy-options]
user@host# set policy statement stop-pim-register-msg-dr then reject
```

5. Assign the policy.

```
[edit]
user@host# set dr-register-policy stop-pim-register-msg-dr
```

Results From configuration mode, confirm your configuration by entering the **show policy-options** and **show protocols** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show policy-options
policy-statement stop-pim-register-msg-dr {
  from {
    route-filter 224.2.2.2/32 exact;
    source-address-filter 20.20.20.1/32 exact;
```

```
    }  
    then reject;  
  }  
[edit]  
user@host# show protocols  
pim {  
  rp {  
    dr-register-policy stop-pim-register-msg-dr;  
  }  
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying SAP and SDP Addresses and Ports on page 124](#)
- [Verifying the IGMP Version on page 124](#)
- [Verifying the PIM Mode and Interface Configuration on page 124](#)
- [Verifying the PIM RP Configuration on page 124](#)

Verifying SAP and SDP Addresses and Ports

Purpose Verify that SAP and SDP are configured to listen on the correct group addresses and ports.

Action From operational mode, enter the **show sap listen** command.

Verifying the IGMP Version

Purpose Verify that IGMP version 2 is configured on all applicable interfaces.

Action From operational mode, enter the **show igmp interface** command.

Verifying the PIM Mode and Interface Configuration

Purpose Verify that PIM sparse mode is configured on all applicable interfaces.

Action From operational mode, enter the **show pim interfaces** command.

Verifying the PIM RP Configuration

Purpose Verify that the PIM RP is statically configured with the correct IP address.

Action From operational mode, enter the **show pim rps** command.

Filtering Incoming PIM Join Messages

Multicast scoping controls the propagation of multicast messages. Whereas multicast scoping prevents the actual multicast data packets from flowing in or out of an interface,

PIM join filters prevent a state from being created in a router. A state—the (*,G) or (S,G) entries—is the information used for forwarding unicast or multicast packets. Using PIM join filters prevents the transport of multicast traffic across a network and the dropping of packets at a scope at the edge of the network. Also, PIM join filters reduce the potential for denial-of-service (DoS) attacks and PIM state explosion—large numbers of PIM join messages forwarded to each router on the rendezvous-point tree (RPT), resulting in memory consumption.

To use PIM join filters to efficiently restrict multicast traffic from certain source addresses, create and apply the routing policy across all routers in the network.

See [Table 7 on page 125](#) for a list of match conditions.

Table 7: PIM Join Filter Match Conditions

Match Condition	Matches On
interface	Router interface or interfaces specified by name or IP address
neighbor	Neighbor address (the source address in the IP header of the join and prune message)
route-filter	Multicast group address embedded in the join and prune message
source-address-filter	Multicast source address embedded in the join and prune message

The following example shows how to create a PIM join filter. The filter is composed of a route filter and a source address filter—**bad-groups** and **bad-sources**, respectively. the **bad-groups** filter prevents (*,G) or (S,G) join messages from being received for all groups listed. The **bad-sources** filter prevents (S,G) join messages from being received for all sources listed. The **bad-groups** filter and **bad-sources** filter are in two different terms. If route filters and source address filters are in the same term, they are logically ANDed.

To filter incoming PIM join messages:

1. Configure the policy.

```
[edit policy-statement pim-join-filter term bad-groups]
user@host# set from route-filter 224.0.1.2/32 exact
user@host# set from route-filter 239.0.0.0/8 orlonger
user@host# set then reject

[edit policy-statement pim-join-filter term bad-sources]
user@host# set from source-address-filter 10.0.0.0/8 orlonger
user@host# set from source-address-filter 127.0.0.0/8 orlonger
user@host# set then reject

[edit policy-statement pim-join-filter term last]
user@host# set then accept
```

2. Apply one or more policies to routes being imported into the routing table from PIM.

```
[edit protocols pim]
user@host# set import pim-join-filter
```

3. Verify the configuration by checking the output of the **show pim join** and **show policy** commands.

Example: Rejecting Incoming PIM Register Messages on RP Routers

This example shows how to reject incoming PIM register messages on RP routers.

- [Requirements on page 126](#)
- [Overview on page 126](#)
- [Configuration on page 126](#)
- [Verification on page 128](#)

Requirements

Before you begin:

1. Determine whether the router is directly attached to any multicast sources. Receivers must be able to locate these sources.
2. Determine whether the router is directly attached to any multicast group receivers. If receivers are present, IGMP is needed.
3. Determine whether to configure multicast to use sparse, dense, or sparse-dense mode. Each mode has different configuration considerations.
4. Determine the address of the RP if sparse or sparse-dense mode is used.
5. Determine whether to locate the RP with the static configuration, BSR, or auto-RP method.
6. Determine whether to configure multicast to use its own RPF routing table when configuring PIM in sparse, dense, or sparse-dense mode.
7. Configure the SAP and SDP protocols to listen for multicast session announcements. See *Configuring the Session Announcement Protocol*.
8. Configure IGMP. See [“Configuring IGMP” on page 19](#).
9. Configure the PIM static RP. See [“Configuring Static RP” on page 106](#).

Overview

In this example, you configure the group address as **224.1.1.1/32** and the source address in the group as **10.10.10.1/32**. You set the match action to reject PIM register messages and assign reject-pim-register-msg-rp as the policy on the RP.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set policy-options policy-statement reject-pim-register-msg-rp from route-filter
  224.1.1.1/32 exact
```



```

set policy-options policy-statement reject-pim-register-msg-rp from source-address-filter
10.10.10.1/32 exact
set policy-options policy-statement reject-pim-register-msg-rp then reject
set protocols pim rp rp-register-policy reject-pim-register-msg-rp

```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To reject the incoming PIM register messages on an RP router:

1. Configure the policy options.

```

[edit]
user@host# edit policy-options

```
2. Set the group address.

```

[edit policy-options]
user@host# set policy statement reject-pim-register-msg-rp from route-filter
224.1.1.1/32 exact

```
3. Set the source address.

```

[edit policy-options]
user@host# set policy statement reject-pim-register-msg-rp from
source-address-filter 10.10.10.1/32 exact

```
4. Set the match action.

```

[edit policy-options]
user@host# set policy statement reject-pim-register-msg-rp then reject

```
5. Configure the protocol.

```

[edit]
user@host# edit protocols pim rp

```
6. Assign the policy.

```

[edit]
user@host# set rp-register-policy reject-pim-register-msg-rp

```

Results From configuration mode, confirm your configuration by entering the **show policy-options** and **show protocols pim** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```

[edit]
user@host# show policy-options
policy-statement reject-pim-register-msg-rp {
  from {
    route-filter 224.1.1.1/32 exact;
    source-address-filter 10.10.10.1/32 exact;
  }
  then reject;
}
[edit]
user@host# show protocols pim
rp {

```

```
rp-register-policy reject-pim-register-msg-rp;  
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying SAP and SDP Addresses and Ports on page 128](#)
- [Verifying the IGMP Version on page 128](#)
- [Verifying the PIM Mode and Interface Configuration on page 128](#)
- [Verifying the PIM Register Messages on page 128](#)

Verifying SAP and SDP Addresses and Ports

Purpose Verify that SAP and SDP are configured to listen on the correct group addresses and ports.

Action From operational mode, enter the **show sap listen** command.

Verifying the IGMP Version

Purpose Verify that IGMP version 2 is configured on all applicable interfaces.

Action From operational mode, enter the **show igmp interface** command.

Verifying the PIM Mode and Interface Configuration

Purpose Verify that PIM sparse mode is configured on all applicable interfaces.

Action From operational mode, enter the **show pim interfaces** command.

Verifying the PIM Register Messages

Purpose Verify whether the rejected policy on the RP router is enabled.

Action From operational mode, enter the **show policy-options** and **show protocols pim** command.

Configuring Register Message Filters on a PIM RP and DR

PIM register messages are sent to the rendezvous point (RP) by a designated router (DR). When a source for a group starts transmitting, the DR sends unicast PIM register packets to the RP.

Register messages have the following purposes:

- Notify the RP that a source is sending to a group.
- Deliver the initial multicast packets sent by the source to the RP for delivery down the shortest-path tree (SPT).

The PIM RP keeps track of all active sources in a single PIM sparse mode domain. In some cases, you want more control over which sources an RP discovers, or which sources a DR notifies other RPs about. A high degree of control over PIM register messages is provided by RP or DR register message filtering. Message filtering prevents unauthorized groups and sources from registering with an RP router.

You configure RP or DR register message filtering to control the number and location of multicast sources that an RP discovers. You can apply register message filters on a DR to control outgoing register messages, or apply them on an RP to control incoming register messages.

When anycast RP is configured, all RPs in the anycast RP set need to be configured with the same register message filtering policy.

You can configure message filtering globally or for a routing instance. These examples show the global configuration.

To configure an RP filter to drop the register packets for multicast group range 224.1.1.0/24 from source address 10.10.94.2:

1. On the RP, configure the policy.

```
[edit policy-options policy-statement incoming-policy-for-rp from]
user@host# set route-filter 224.1.1.0/24 orlonger
user@host# set source-address-filter 10.10.94.2/32 exact
user@host# set then reject
user@host# exit
```

2. Apply the policy to the RP.

```
[edit protocols pim rp]
user@host# set rp-register-policy incoming-policy-for-rp
user@host# set local address 10.10.10.5
user@host# exit
```

To configure a DR filter to prevent sending register packets for group range 224.1.1.0/24 and source address 10.10.10.1/32:

1. On the DR, configure the policy.

```
[edit policy-options policy-statement outgoing-policy-for-rp]
user@host# set from route-filter 224.1.1.0/24 orlonger
user@host# set from source-address-filter 10.10.10.1/32 exact
user@host# set then reject
user@host# exit
```

2. Apply the policy to the DR.

The static address is the address of the RP to which you do not want the DR to send the filtered register messages.

```
[edit protocols pim rp]
user@host# set dr-register-policy outgoing-policy-for-dr
user@host# set static 10.10.10.3
user@host# exit
```

To configure a policy expression to accept register messages for multicast group 224.1.1.5 but reject those for 224.1.1.1:

1. On the RP, configure the policies.

```
[edit policy-options policy-statement reject_224_1_1_1]
user@host# set from route-filter 224.1.1.0/24 orlonger
user@host# set from source-address-filter 10.10.94.2/32 exact
user@host# set then reject
user@host# exit

[edit policy-options policy-statement accept_224_1_1_5]
user@host# set term one from route-filter 224.1.1.5/32 exact
user@host# set term one from source-address-filter 10.10.94.2/32 exact
user@host# set term one then accept
user@host# set term two then reject
user@host# exit
```

2. Apply the policies to the RP.

```
[edit protocols pim rp]
user@host# set rp-register-policy [ reject_224_1_1_1 | accept_224_1_1_5 ]
user@host# set local address 10.10.10.5
```

To monitor the operation of the filters, run the **show pim statistics** command. The command output contains the following fields related to filtering:

- RP Filtered Source
- Rx Joins/Prunes filtered
- Tx Joins/Prunes filtered
- Rx Register msgs filtering drop
- Tx Register msgs filtering drop

Related Documentation

- [Configuring PIM Auto-RP on page 99](#)
- [Configuring PIM Bootstrap Router on page 113](#)
- [Configuring PIM Dense Mode on page 93](#)
- [Configuring a Designated Router for PIM on page 90](#)
- *Example: Configuring Nonstop Active Routing for PIM*
- *Examples: Configuring PIM RPT and SPT Cutover*
- [Configuring PIM Sparse-Dense Mode on page 96](#)
- [Configuring PIM and the Bidirectional Forwarding Detection \(BFD\) Protocol on page 131](#)
- [Configuring Basic PIM Settings on page 77](#)

CHAPTER 8

Rapidly Detecting Communication Failures with PIM and BFD Protocol

- [Configuring PIM and the Bidirectional Forwarding Detection \(BFD\) Protocol on page 131](#)

Configuring PIM and the Bidirectional Forwarding Detection (BFD) Protocol

- [Understanding Bidirectional Forwarding Detection Authentication for PIM on page 131](#)
- [Configuring BFD for PIM on page 133](#)
- [Configuring BFD Authentication for PIM on page 134](#)
- [Example: Configuring BFD Liveness Detection for PIM IPv6 on page 137](#)

Understanding Bidirectional Forwarding Detection Authentication for PIM

Bidirectional Forwarding Detection (BFD) enables rapid detection of communication failures between adjacent systems. By default, authentication for BFD sessions is disabled. However, when you run BFD over Network Layer protocols, the risk of service attacks can be significant. We strongly recommend using authentication if you are running BFD over multiple hops or through insecure tunnels.



NOTE: Beginning with Junos OS Release 9.6, Junos OS supports authentication for BFD sessions running over PIM. BFD authentication is only supported in the Canada and United States version of the Junos OS image and is not available in the export version.

You authenticate BFD sessions by specifying an authentication algorithm and keychain, and then associating that configuration information with a security authentication keychain using the keychain name.

The following sections describe the supported authentication algorithms, security keychains, and level of authentication that can be configured:

- [BFD Authentication Algorithms on page 132](#)
- [Security Authentication Keychains on page 132](#)
- [Strict Versus Loose Authentication on page 133](#)

BFD Authentication Algorithms

Junos OS supports the following algorithms for BFD authentication:

- **simple-password**—Plain-text password. One to 16 bytes of plain text are used to authenticate the BFD session. One or more passwords can be configured. This method is the least secure and should be used only when BFD sessions are not subject to packet interception.
- **keyed-md5**—Keyed Message Digest 5 hash algorithm for sessions with transmit and receive intervals greater than 100 ms. To authenticate the BFD session, keyed MD5 uses one or more secret keys (generated by the algorithm) and a sequence number that is updated periodically. With this method, packets are accepted at the receiving end of the session if one of the keys matches and the sequence number is greater than or equal to the last sequence number received. Although more secure than a simple password, this method is vulnerable to replay attacks. Increasing the rate at which the sequence number is updated can reduce this risk.
- **meticulous-keyed-md5**—Meticulous keyed Message Digest 5 hash algorithm. This method works in the same manner as keyed MD5, but the sequence number is updated with every packet. Although more secure than keyed MD5 and simple passwords, this method might take additional time to authenticate the session.
- **keyed-sha-1**—Keyed Secure Hash Algorithm 1 for sessions with transmit and receive intervals greater than 100 ms. To authenticate the BFD session, keyed SHA uses one or more secret keys (generated by the algorithm) and a sequence number that is updated periodically. The key is not carried within the packets. With this method, packets are accepted at the receiving end of the session if one of the keys matches and the sequence number is greater than the last sequence number received.
- **meticulous-keyed-sha-1**—Meticulous keyed Secure Hash Algorithm 1. This method works in the same manner as keyed SHA, but the sequence number is updated with every packet. Although more secure than keyed SHA and simple passwords, this method might take additional time to authenticate the session.



NOTE: Nonstop active routing (NSR) is not supported with meticulous-keyed-md5 and meticulous-keyed-sha-1 authentication algorithms. BFD sessions using these algorithms might go down after a switchover.

Security Authentication Keychains

The security authentication keychain defines the authentication attributes used for authentication key updates. When the security authentication keychain is configured and associated with a protocol through the keychain name, authentication key updates can occur without interrupting routing and signaling protocols.

The authentication keychain contains one or more keychains. Each keychain contains one or more keys. Each key holds the secret data and the time at which the key becomes valid. The algorithm and keychain must be configured on both ends of the BFD session,

and they must match. Any mismatch in configuration prevents the BFD session from being created.

BFD allows multiple clients per session, and each client can have its own keychain and algorithm defined. To avoid confusion, we recommend specifying only one security authentication keychain.

Strict Versus Loose Authentication

By default, strict authentication is enabled, and authentication is checked at both ends of each BFD session. Optionally, to smooth migration from nonauthenticated sessions to authenticated sessions, you can configure *loose checking*. When loose checking is configured, packets are accepted without authentication being checked at each end of the session. This feature is intended for transitional periods only.

Configuring BFD for PIM

The Bidirectional Forwarding Detection (BFD) Protocol is a simple hello mechanism that detects failures in a network. BFD works with a wide variety of network environments and topologies. A pair of routing devices exchanges BFD packets. Hello packets are sent at a specified, regular interval. A neighbor failure is detected when the routing device stops receiving a reply after a specified interval. The BFD failure detection timers have shorter time limits than the Protocol Independent Multicast (PIM) hello hold time, so they provide faster detection.

The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. The lower the BFD failure detection timer value, the faster the failure detection and vice versa. For example, the timers can adapt to a higher value if the adjacency fails (that is, the timer detects failures more slowly). Or a neighbor can negotiate a higher value for a timer than the configured value. The timers adapt to a higher value when a BFD session flap occurs more than three times in a span of 15 seconds. A back-off algorithm increases the receive (Rx) interval by two if the local BFD instance is the reason for the session flap. The transmission (Tx) interval is increased by two if the remote BFD instance is the reason for the session flap. You can use the **clear bfd adaptation** command to return BFD interval timers to their configured values. The **clear bfd adaptation** command is hitless, meaning that the command does not affect traffic flow on the routing device.

You must specify the minimum transmit and minimum receive intervals to enable BFD on PIM.

To enable failure detection:

1. Configure the interface globally or in a routing instance.

This example shows the global configuration.

```
[edit protocols pim]
user@host# edit interface fe-1/0/0.0 family inet bfd-liveness-detection
```

2. Configure the minimum transmit interval.

This is the minimum interval after which the routing device transmits hello packets to a neighbor with which it has established a BFD session. Specifying an interval smaller than 300 ms can cause undesired BFD flapping.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set transmit-interval 350
```

3. Configure the minimum interval after which the routing device expects to receive a reply from a neighbor with which it has established a BFD session.

Specifying an interval smaller than 300 ms can cause undesired BFD flapping.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set minimum-receive-interval 350
```

4. (Optional) Configure other BFD settings.

As an alternative to setting the receive and transmit intervals separately, configure one interval for both.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set minimum-interval 350
```

5. Configure the threshold for the adaptation of the BFD session detection time.

When the detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set detection-time threshold 800
```

6. Configure the number of hello packets not received by a neighbor that causes the originating interface to be declared down.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set multiplier 50
```

7. Configure the BFD version.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set version 1
```

8. Specify that BFD sessions should not adapt to changing network conditions.

We recommend that you not disable BFD adaptation unless it is preferable not to have BFD adaptation enabled in your network.

```
[edit protocols pim interface fe-1/0/0.0 family inet bfd-liveness-detection]
user@host# set no-adaptation
```

9. Verify the configuration by checking the output of the **show bfd session** command.

Configuring BFD Authentication for PIM

Beginning with Junos OS Release 9.6, you can configure authentication for Bidirectional Forwarding Detection (BFD) sessions running over Protocol Independent Multicast (PIM). Routing instances are also supported. The following steps are needed to configure authentication on a BFD session:

1. Specify the BFD authentication algorithm for the PIM protocol.
2. Associate the authentication keychain with the PIM protocol.
3. Configure the related security authentication keychain.

The following sections provide instructions for configuring and viewing BFD authentication on PIM:

- [Configuring BFD Authentication Parameters on page 135](#)
- [Viewing Authentication Information for BFD Sessions on page 136](#)

Configuring BFD Authentication Parameters

BFD authentication is only supported in the Canada and United States version of the Junos OS image and is not available in the export version.

To configure BFD authentication:

1. Specify the algorithm (**keyed-md5**, **keyed-sha-1**, **meticulous-keyed-md5**, **meticulous-keyed-sha-1**, or **simple-password**) to use for BFD authentication on a PIM route or routing instance.

```
[edit protocols pim]
user@host# set interface ge-0/1/5 family inet bfd-liveness-detection authentication
algorithm keyed-sha-1
```



NOTE: Nonstop active routing (NSR) is not supported with the **meticulous-keyed-md5** and **meticulous-keyed-sha-1** authentication algorithms. BFD sessions using these algorithms might go down after a switchover.

2. Specify the keychain to be used to associate BFD sessions on the specified PIM route or routing instance with the unique security authentication keychain attributes.

The keychain you specify must match the keychain name configured at the **[edit security authentication key-chains]** hierarchy level.

```
[edit protocols pim]
user@host# set interface ge-0/1/5 family inet bfd-liveness-detection authentication
keychain bfd-pim
```



NOTE: The algorithm and keychain must be configured on both ends of the BFD session, and they must match. Any mismatch in configuration prevents the BFD session from being created.

3. Specify the unique security authentication information for BFD sessions:
 - The matching keychain name as specified in Step 2.
 - At least one key, a unique integer between 0 and 63. Creating multiple keys allows multiple clients to use the BFD session.
 - The secret data used to allow access to the session.
 - The time at which the authentication key becomes active, in the format *yyyy-mm-dd.hh:mm:ss*.

```
[edit security]
user@host# set authentication-key-chains key-chain bfd-pim key 53 secret
$9$ggaJDmPQ6/tJgF/AtREVsyPsnCtUHm start-time 2009-06-14.10:00:00
```

4. (Optional) Specify loose authentication checking if you are transitioning from nonauthenticated sessions to authenticated sessions.

```
[edit protocols pim]
user@host# set interface ge-0/1/5 family inet bfd-liveness-detection authentication
loose-check
```

5. (Optional) View your configuration by using the **show bfd session detail** or **show bfd session extensive** command.
6. Repeat these steps to configure the other end of the BFD session.

Viewing Authentication Information for BFD Sessions

You can view the existing BFD authentication configuration by using the **show bfd session detail** and **show bfd session extensive** commands.

The following example shows BFD authentication configured for the **ge-0/1/5** interface. It specifies the keyed SHA-1 authentication algorithm and a keychain name of **bfd-pim**. The authentication keychain is configured with two keys. Key 1 contains the secret data "**\$9\$ggaJDmPQ6/tJgF/AtREVsyPsnCtUHm**" and a start time of June 1, 2009, at 9:46:02 AM PST. Key 2 contains the secret data "**\$9\$a5jiKW9l.reP38ny.TszF2/9**" and a start time of June 1, 2009, at 3:29:20 PM PST.

```
[edit protocols pim]
interface ge-0/1/5 {
  family inet {
    bfd-liveness-detection {
      authentication {
        key-chain bfd-pim;
        algorithm keyed-sha-1;
      }
    }
  }
}
[edit security]
authentication key-chains {
  key-chain bfd-pim {
    key 1 {
      secret "$9$ggaJDmPQ6/tJgF/AtREVsyPsnCtUHm";
      start-time "2009-6-1.09:46:02 -0700";
    }
    key 2 {
      secret "$9$a5jiKW9l.reP38ny.TszF2/9";
      start-time "2009-6-1.15:29:20 -0700";
    }
  }
}
```

If you commit these updates to your configuration, you see output similar to the following example. In the output for the **show bfd session detail** command, **Authenticate** is displayed to indicate that BFD authentication is configured. For more information about the

configuration, use the **show bfd session extensive** command. The output for this command provides the keychain name, the authentication algorithm and mode for each client in the session, and the overall BFD authentication configuration status, keychain name, and authentication algorithm and mode.

show bfd session detail

```
user@host# show bfd session detail
```

Address	State	Interface	Detect Time	Transmit Interval	Multiplier
50.0.0.2	Up	ge-0/1/5.0	0.900	0.300	3

Client PIM, TX interval 0.300, RX interval 0.300, **Authenticate**
 Session up time 3d 00:34
 Local diagnostic None, remote diagnostic NbrSignal
 Remote state Up, version 1
 Replicated

show bfd session extensive

```
user@host# show bfd session extensive
```

Address	State	Interface	Detect Time	Transmit Interval	Multiplier
50.0.0.2	Up	ge-0/1/5.0	0.900	0.300	3

Client PIM, TX interval 0.300, RX interval 0.300, **Authenticate**
keychain bfd-pim, algo keyed-sha-1, mode strict
 Session up time 00:04:42
 Local diagnostic None, remote diagnostic NbrSignal
 Remote state Up, version 1
 Replicated
 Min async interval 0.300, min slow interval 1.000
 Adaptive async TX interval 0.300, RX interval 0.300
 Local min TX interval 0.300, minimum RX interval 0.300, multiplier 3
 Remote min TX interval 0.300, min RX interval 0.300, multiplier 3
 Local discriminator 2, remote discriminator 2
 Echo mode disabled/inactive
Authentication enabled/active, keychain bfd-pim, algo keyed-sha-1, mode strict

Example: Configuring BFD Liveness Detection for PIM IPv6

This example shows how to configure Bidirectional Forwarding Detection (BFD) liveness detection for IPv6 interfaces configured for the Protocol Independent Multicast (PIM) topology. BFD is a simple hello mechanism that detects failures in a network.

The following steps are needed to configure BFD liveness detection:

1. Configure the interface.
2. Configure the related security authentication keychain.
3. Specify the BFD authentication algorithm for the PIM protocol.
4. Configure PIM, associating the authentication keychain with the desired protocol.
5. Configure BFD authentication for the routing instance.



NOTE: You must perform these steps on both ends of the BFD session.

- [Requirements on page 138](#)
- [Overview on page 138](#)
- [Configuration on page 139](#)
- [Verification on page 142](#)

Requirements

This example uses the following hardware and software components:

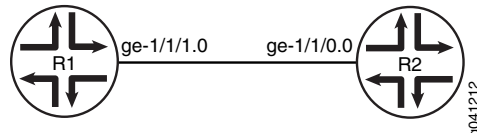
- Two peer routers.
- Junos OS 12.2 or later.

Overview

In this example, Device R1 and Device R2 are peers. Each router runs PIM, connected over a common medium.

[Figure 18 on page 138](#) shows the topology used in this example.

Figure 18: BFD Liveness Detection for PIM IPv6 Topology



Assume that the routers initialize. No BFD session is yet established. For each router, PIM informs the BFD process to monitor the IPv6 address of the neighbor that is configured in the routing protocol. Addresses are not learned dynamically and must be configured.

Configure the IPv6 address and BFD liveness detection at the `[edit protocols pim]` hierarchy level for each router.

```
[edit protocols pim]
user@host# set interface interface-name family inet6 bfd-liveness-detection
```

Configure BFD liveness detection for the routing instance at the `[edit routing-instances instance-name protocols pim interface all family inet6]` hierarchy level (here, the *instance-name* is *instance1*):

```
[edit routing-instances instance1 protocols pim]
user@host# set bfd-liveness-detection
```

You will also configure the authentication algorithm and authentication keychain values for BFD.

In a BFD-configured network, when a client launches a BFD session with a peer, BFD begins sending slow, periodic BFD control packets that contain the interval values that you specified when you configured the BFD peers. This is known as the initialization state.

BFD does not generate any up or down notifications in this state. When another BFD interface acknowledges the BFD control packets, the session moves into an up state and begins to more rapidly send periodic control packets. If a data path failure occurs and BFD does not receive a control packet within the configured amount of time, the data path is declared down and BFD notifies the BFD client. The BFD client can then perform the necessary actions to reroute traffic. This process can be different for different BFD clients.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
Device R1
set interfaces ge-0/1/5 unit 0 description toRouter2
set interfaces ge-0/1/5 unit 0 family inet6
set interfaces ge-0/1/5 unit 0 family inet6 address e80::21b:c0ff:fed5:e4dd
set protocols pim interface ge-0/1/5 family inet6 bfd-liveness-detection authentication
  algorithm keyed-sha-1
set protocols pim interface ge-0/1/5 family inet6 bfd-liveness-detection authentication
  key-chain bfd-pim
set routing-instances instance1 protocols pim interface all family inet6
  bfd-liveness-detection authentication algorithm keyed-sha-1
set routing-instances instance1 protocols pim interface all family inet6
  bfd-liveness-detection authentication key-chain bfd-pim
set security authentication key-chain bfd-pim key 1 secret
  "$9$ggaJDmPQ6/tJgF/AtREVsyPsnCtUHM"
set security authentication key-chain bfd-pim key 1 start-time "2012-01-01.09:46:02
-0700"
set security authentication key-chain bfd-pim key 2 secret
  "$9$a5jiKW9l.reP38ny.TszF2/9"
set security authentication key-chain bfd-pim key 2 start-time "2012-01-01.15:29:20
-0700"

Device R2
set interfaces ge-1/1/0 unit 0 description toRouter1
set interfaces ge-1/1/0 unit 0 family inet6 address e80::21b:c0ff:fed5:e5dd
set protocols pim interface ge-1/1/0 family inet6 bfd-liveness-detection authentication
  algorithm keyed-sha-1
set protocols pim interface ge-1/1/0 family inet6 bfd-liveness-detection authentication
  key-chain bfd-pim
set routing-instances instance1 protocols pim interface all family inet6
  bfd-liveness-detection authentication algorithm keyed-sha-1
set routing-instances instance1 protocols pim interface all family inet6
  bfd-liveness-detection authentication key-chain bfd-pim
set security authentication key-chain bfd-pim key 1 secret
  "$9$ggaJDmPQ6/tJgF/AtREVsyPsnCtUHM"
set security authentication key-chain bfd-pim key 1 start-time "2012-01-01.09:46:02
-0700"
set security authentication key-chain bfd-pim key 2 secret
  "$9$a5jiKW9l.reP38ny.TszF2/9"
set security authentication key-chain bfd-pim key 2 start-time "2012-01-01.15:29:20
-0700"
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure BFD liveness detection for PIM IPv6 interfaces on Device R1:



NOTE: This procedure is for Device R1. Repeat this procedure for Device R2, after modifying the appropriate interface names, addresses, and any other parameters.

1. Configure the interface, using the **inet6** statement to specify that this is an IPv6 address.

```
[edit interfaces]
user@R1# set ge-0/1/5 unit 0 description toRouter2
user@R1# set ge-0/1/5 unit 0 family inet6 address e80::21b:c0ff:fed5:e4dd
```

2. Specify the BFD authentication algorithm and keychain for the PIM protocol.

The keychain is used to associate BFD sessions on the specified PIM route or routing instance with the unique security authentication keychain attributes. This keychain name should match the keychain name configured at the **[edit security authentication]** hierarchy level.

```
[edit protocols]
user@R1# set pim interface ge-0/1/5.0 family inet6 bfd-liveness-detection
authentication algorithm keyed-sha-1
user@R1# set pim interface ge-0/1/5 family inet6 bfd-liveness-detection
authentication key-chain bfd-pim
```



NOTE: The algorithm and keychain must be configured on both ends of the BFD session, and they must match. Any mismatch in configuration prevents the BFD session from being created.

3. Configure a routing instance (here, **instance1**), specifying BFD authentication and associating the security authentication algorithm and keychain.

```
[edit routing-instances]
user@R1# set instance1 protocols pim interface all family inet6
bfd-liveness-detection authentication algorithm keyed-sha-1
user@R1# set instance1 protocols pim interface all family inet6
bfd-liveness-detection authentication key-chain bfd-pim
```

4. Specify the unique security authentication information for BFD sessions:
 - The matching keychain name as specified in Step 2.
 - At least one key, a unique integer between **0** and **63**. Creating multiple keys allows multiple clients to use the BFD session.

- The secret data used to allow access to the session.
- The time at which the authentication key becomes active, in the format YYYY-MM-DD.hh:mm:ss.

```
[edit security authentication]
user@R1# set key-chain bfd-pim key 1 secret
"$9$ggaJDmPQ6/tJgF/AtREVsyPsnCtUHM"
user@R1# set key-chain bfd-pim key 1 start-time "2012-01-01.09:46:02 -0700"
user@R1# set key-chain bfd-pim key 2 secret "$9$a5jiKW9L.reP38ny.TszF2/9"
user@R1# set key-chain bfd-pim key 2 start-time "2012-01-01.15:29:20 -0700"
```

Results

Confirm your configuration by issuing the **show interfaces**, **show protocols**, **show routing-instances**, and **show security** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@R1# show interfaces
ge-0/1/5 {
  unit 0 {
    description toRouter2;
    family inet6 {
      address e80::21b:c0ff:fed5:e4dd {
      }
    }
  }
}

user@R1# show protocols
pim {
  interface ge-0/1/5.0 {
    family inet6;
    bfd-liveness-detection {
      authentication {
        algorithm keyed-sha-1;
        key-chain bfd-pim;
      }
    }
  }
}

user@R1# show routing-instances
instance1 {
  protocols {
    pim {
      interface all {
        family inet6 {
          bfd-liveness-detection {
            authentication {
              algorithm keyed-sha-1;
              key-chain bfd-pim;
            }
          }
        }
      }
    }
  }
}
```

```

    }
  }
}

user@R1# show security
authentication {
  key-chain bfd-pim {
    key 1 {
      secret "$9$ggaJDmPQ6/tJgF/AtREVsyPsnCtUHm";
      start-time "2012-01-01.09:46:02 -0700";
    }
    key 2 {
      secret "$9$a5jiKW9l.reP38ny.TszF2/9";
      start-time "2012-01-01.15:29:20 -0700";
    }
  }
}

```

Verification

Confirm that the configuration is working properly.

Verifying the BFD Session

Purpose Verify that BFD liveness detection is enabled.

Action user@R1# run `show pim neighbors detail`

Instance: PIM.master

Interface: ge-0/1/5.0

Address: fe80::21b:c0ff:fed5:e4dd, IPv6, PIM v2, Mode: Sparse, sg Join Count: 0, tsg Join Count: 0

Hello Option Holdtime: 65535 seconds

Hello Option DR Priority: 1

Hello Option Generation ID: 1417610277

Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Join Suppression supported

Address: fe80::21b:c0ff:fedc:28dd, IPv6, PIM v2, sg Join Count: 0, tsg Join Count: 0

Secondary address: beef::2

BFD: Enabled, Operational state: Up

Hello Option Holdtime: 105 seconds 80 remaining

Hello Option DR Priority: 1

Hello Option Generation ID: 1648636754

Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Join Suppression supported

Meaning The display from the `show pim neighbors detail` command shows **BFD: Enabled, Operational state: Up**, indicating that BFD is operating between the two PIM neighbors. For additional information about the BFD session (including the session ID number), use the `show bfd session extensive` command.

Related Documentation

- [Configuring Basic PIM Settings on page 77](#)

- *Example: Configuring BFD for BGP*
- *Example: Configuring BFD Authentication for BGP*

PART 4

Configuring Multicast Routing Protocols

- [Connecting Routing Domains Using MSDP on page 147](#)

CHAPTER 9

Connecting Routing Domains Using MSDP

- [Configuring Multiple Instances of MSDP on page 147](#)

Configuring Multiple Instances of MSDP

MSDP instances are supported only for VRF instance types. You can configure multiple instances of MSDP to support multicast over VPNs.

To configure multiple instances of MSDP, include the following statements:

```
routing-instances {  
  routing-instance-name {  
    interface interface-name;  
    instance-type vrf;  
    route-distinguisher (as-number:number | ip-address:number);  
    vrf-import [ policy-names ];  
    vrf-export [ policy-names ];  
    protocols {  
      msdp {  
        ... msdp-configuration ...  
      }  
    }  
  }  
}
```

You can include the statements at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols]

Related Documentation

- [Example: Configuring MSDP in a Routing Instance](#)
- [Junos OS MPLS Applications Library for Routing Devices](#)
- [Junos OS VPNs Library for Routing Devices](#)

PART 5

Configuring Multicast VPNs

- [Configuring PIM Join Load Balancing on page 151](#)

Configuring PIM Join Load Balancing

- [PIM Join Load Balancing on Multipath MVPN Routes Overview on page 151](#)

PIM Join Load Balancing on Multipath MVPN Routes Overview

A multicast virtual private network (MVPN) is a technology to deploy the multicast service in an existing MPLS/BGP VPN.

The two main MVPN services are:

- Dual PIM MVPNs (also referred to as Draft-Rosen)
- Multiprotocol BGP-based MVPNs (also referred to as next-generation)

Next-generation MVPNs constitute the next evolution after the Draft-Rosen MVPN and provide a simpler solution for administrators who want to configure multicast over Layer 3 VPNs. A Draft-Rosen MVPN uses Protocol Independent Multicast (PIM) for customer multicast (C-multicast) signaling, and a next-generation MVPN uses BGP for C-multicast signaling.

Multipath routing in an MVPN is applied to make data forwarding more robust against network failures and to minimize shared backup capacities when resilience against network failures is required.

By default, PIM join messages are sent toward a source based on the reverse path forwarding (RPF) routing table check. If there is more than one equal-cost path toward the source [S, G] or rendezvous point (RP) [* G], then one upstream interface is used to send the join messages. The upstream path can be:

- A single active external BGP (EBGP) path when both EBGP and internal BGP (IBGP) paths are present.
- A single active IBGP path when there is no EBGP path present.

With the introduction of the multipath PIM join load-balancing feature, customer PIM (C-PIM) join messages are load-balanced in the following ways:

- In the case of a Draft-Rosen MVPN, unequal EBGP and IBGP paths are utilized.
- In the case of next-generation MVPN:
 - Available IBGP paths are utilized when no EBGP path is present.

- Available EGBP paths are utilized when both EGBP and IGBP paths are present.

This feature is applicable to IPv4 C-PIM join messages over the Layer 3 MVPN service.

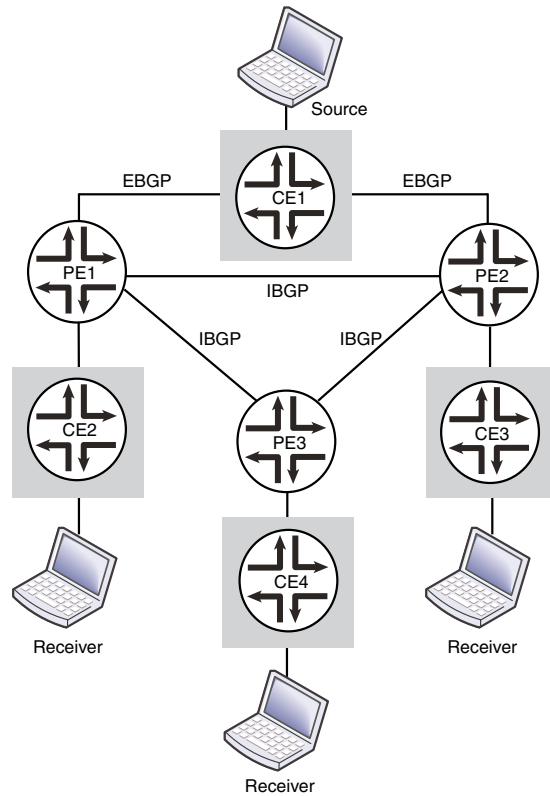
By default, a customer source (C-S) or a customer RP (C-RP) is considered remote if the active **rt_entry** is a secondary route and the primary route is present in a different routing instance. Such determination is being done without taking into consideration the (C-*;G) or (C-S,G) state for which the check is being performed. The multipath PIM join load-balancing feature determines if a source (or RP) is remote by taking into account the associated (C-*;G) or (C-S,G) state.

When the provider network does not have provider edge (PE) routing devices with the multipath PIM join load-balancing feature enabled, hash-based join load balancing is used. Although the decision to configure this feature does not impact PIM or overall system performance, network performance can be affected temporarily, if the feature is not enabled.

With hash-based join load balancing, adding new PE routing devices to the candidate upstream toward the C-S or C-RP results in C-PIM join messages being redistributed to new upstream paths. If the number of join messages is large, network performance is impacted because of join messages being sent to the new RPF neighbor and prune messages being sent to the old RPF neighbor. In next-generation MVPN, this results in BGP C-multicast data messages being withdrawn from old upstream paths and advertised on new upstream paths, impacting network performance.

In Figure 19 on page 153, PE1 and PE2 are the upstream PE routing devices. Router PE1 learns route Source from EGBP and IBGP peers—the customer edge CE1 router and the PE2 router, respectively.

Figure 19: PIM Join Load Balancing



- If the PE routing devices run the Draft-Rosen MVPN, the PE1 router distributes C-PIM join messages between the EGBP path to the CE1 router and the IBGP path to the PE2 router. The join messages on the IBGP path are sent over a multicast tunnel interface through which the PE routing devices establish C-PIM adjacency with each other.

If a PE routing device loses one or all EGBP paths toward the source (or RP), the C-PIM join messages that were previously using the EGBP path are moved to a multicast tunnel interface, and the RPF neighbor on the multicast tunnel interface is selected based on a hash mechanism.

On discovering the first EGBP path toward the source (or RP), only new join messages get load-balanced across EGBP and IBGP paths, whereas the existing join messages on the multicast tunnel interface remain unaffected.

- If the PE routing devices run the next-generation MVPN, the PE1 router sends C-PIM join messages directly to the CE1 router over the EGBP path. There is no C-PIM adjacency between the PE1 and PE2 routers. Router PE3 distributes the C-PIM join messages between the two IBGP paths to PE1 and PE2. The Bitwise-XOR hash algorithm is used to send the C-multicast data according to Internet draft draft-ietf-l3vpn-2547bis-mcast-bgp, *BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs*.

Because the multipath PIM join load-balancing feature in a Draft-Rosen MVPN utilizes unequal EGBP and IBGP paths to the destination, loops can be created when forwarding unicast packets to the destination. To avoid or break such loops:

- Traffic arriving from a core or master instance should not be forwarded back to the core facing interfaces.
- A single multicast tunnel interface should either be selected as the upstream interface or the downstream interface.
- An upstream or downstream multicast tunnel interface should point to a non-multicast tunnel interface.

As a result of the loop avoidance mechanism, join messages arriving from an EGBP path get load-balanced across EIBGP paths as expected, whereas join messages from an IBGP path are constrained to choose the EGBP path only.

In [Figure 19 on page 153](#), if the CE2 host sends unicast data traffic to the CE1 host, the PE1 router could send the multicast flow to the PE2 router over the MPLS core due to traffic load balancing. A data forwarding loop is prevented by ensuring that PE2 does not forward traffic back on the MPLS core because of the load-balancing algorithm.

In the case of C-PIM join messages, assuming that both the CE2 host and the CE3 host are interested in receiving traffic from the source (S, G), and if both PE1 and PE2 choose each other as the RPF neighbor toward the source, then a multicast tree cannot be formed completely. This feature implements mechanisms to prevent such join loops in the multicast control plane in a Draft-Rosen MVPN scenario.

**NOTE:**

Disruption of multicast traffic or creation of join loops can occur, resulting in a multicast distribution tree (MDT) not being formed properly due to one of the following reasons:

- During a graceful Routing Engine switchover (GRES), the EIBGP path selection for C-PIM join messages can vary, because the upstream interface selection is performed again for the new Routing Engine based on the join messages it receives from the CE and PE neighbors. This can lead to disruption of multicast traffic depending on the number of join messages received and the load on the network at the time of the graceful restart. However, nonstop active routing (NSR) is not supported and has no impact on the multicast traffic in a Draft-Rosen MVPN scenario.
 - Any PE routing device in the provider network is running another vendor's implementation that does not apply the same hashing algorithm implemented in this feature.
 - The multipath PIM join load-balancing feature has not been configured properly.
-

Related Documentation

- *Use Case for PIM Join Load Balancing*

- *Example: Configuring PIM Join Load Balancing on Draft-Rosen Multicast VPN*
- *Example: Configuring PIM Join Load Balancing On Next-Generation Multicast VPN*

PART 6

Configuring General Multicast Options

- [Enabling Multicast Between Layer 2 and Layer 3 Devices Using Snooping on page 159](#)

Enabling Multicast Between Layer 2 and Layer 3 Devices Using Snooping

- [PIM Snooping for VPLS on page 159](#)

PIM Snooping for VPLS

- [Understanding PIM Snooping for VPLS on page 159](#)
- [Example: Configuring PIM Snooping for VPLS on page 160](#)

Understanding PIM Snooping for VPLS

There are two ways to direct PIM control packets:

- By the use of PIM snooping
- By the use of PIM proxying

PIM snooping configures a device to examine and operate only on PIM hello and join/prune packets. A PIM snooping device snoops PIM hello and join/prune packets on each interface to find interested multicast receivers and populates the multicast forwarding tree with this information. PIM snooping differs from PIM proxying in that both PIM hello and join/prune packets are transparently flooded in the VPLS as opposed to the flooding of only hello packets in the case of PIM proxying. PIM snooping is configured on PE routers connected through pseudowires. PIM snooping ensures that no new PIM packets are generated in the VPLS, with the exception of PIM messages sent through LDP on pseudowires.



NOTE: In the VPLS documentation, the word *router* in terms such as *PE router* is used to refer to any device that provides routing functions.

A device that supports PIM snooping snoops hello packets received on attachment circuits. It does not introduce latency in the VPLS core when it forwards PIM join/prune packets.

To configure PIM snooping on a PE router, use the **pim-snooping** statement at the **[edit routing-instances *instance-name* protocols]** hierarchy level:

```
routing-instances {
  customer {
    instance-type vpls;
    ...
    protocols {
      pim-snooping {
        traceoptions {
          file pim.log size 10m;
          flag all;
          flag timer disable;
        }
      }
    }
  }
}
```

“[Example: Configuring PIM Snooping for VPLS](#)” on [page 160](#) explains the PIM snooping method. The use of the PIM proxying method is not discussed here and is outside the scope of this document. For more information about PIM proxying, see [PIM Snooping over VPLS](#).

Example: Configuring PIM Snooping for VPLS

This example shows how to configure PIM snooping in a virtual private LAN service (VPLS) to restrict multicast traffic to interested devices.

- [Requirements on page 160](#)
- [Overview on page 160](#)
- [Configuration on page 161](#)
- [Verification on page 167](#)

Requirements

This example uses the following hardware and software components:

- M Series Multiservice Edge Routers (M7i and M10i with Enhanced CFEB, M120, and M320 with E3 FPCs) or MX Series 3D Universal Edge Routers (MX80, MX240, MX480, and MX960)
- Junos OS Release 13.2 or later

Overview

The following example shows how to configure PIM snooping to restrict multicast traffic to interested devices in a VPLS.



NOTE: This example demonstrates PIM snooping by the use of a PIM snooping device to restrict multicast traffic. The use of the PIM proxying method to achieve PIM snooping is out of the scope of this document and is yet to be implemented in Junos OS.

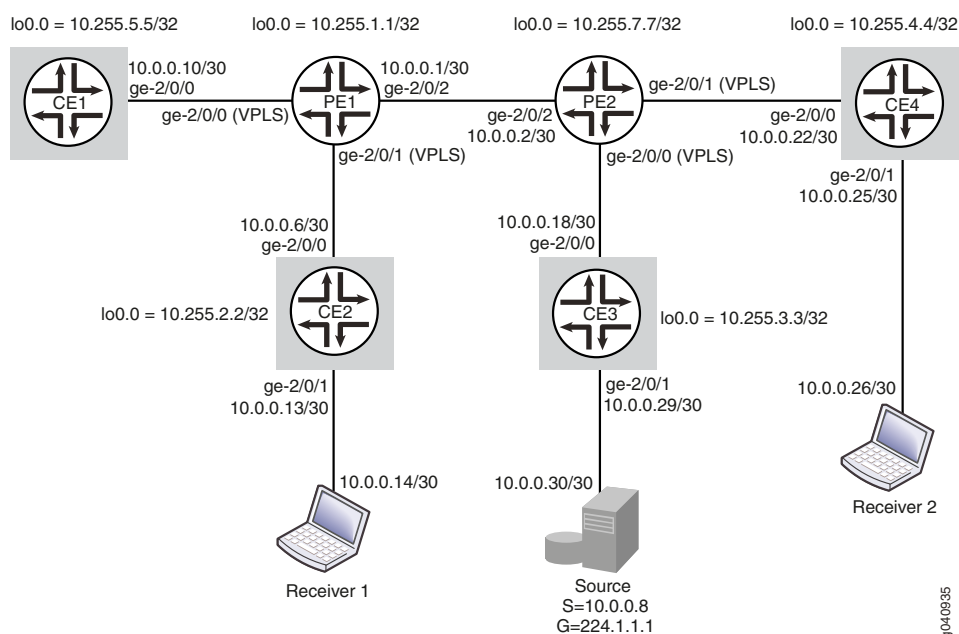
Topology

In this example, two PE routers are connected to each other through a pseudowire connection. Router PE1 is connected to Routers CE1 and CE2. A multicast receiver is attached to Router CE2. Router PE2 is connected to Routers CE3 and CE4. A multicast source is connected to Router CE3, and a second multicast receiver is attached to Router CE4.

PIM snooping is configured on Routers PE1 and PE2. Hence, data sent from the multicast source is received only by members of the multicast group.

Figure 20 on page 161 shows the topology used in this example.

Figure 20: PIM Snooping for VPLS



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
Router PE1
set multicast-snooping-options traceoptions file snoop.log size 10m
set interfaces ge-2/0/0 encapsulation ethernet-vpls
set interfaces ge-2/0/0 unit 0 description toCE1
set interfaces ge-2/0/1 encapsulation ethernet-vpls
set interfaces ge-2/0/1 unit 0 description toCE2
set interfaces ge-2/0/2 unit 0 description toPE2
set interfaces ge-2/0/2 unit 0 family inet address 10.0.0.1/30
set interfaces ge-2/0/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.1.1/32
set routing-options router-id 10.255.1.1
```

```
set protocols mpls interface ge-2/0/1.0
set protocols bgp group toPE2 type internal
set protocols bgp group toPE2 local-address 10.255.1.1
set protocols bgp group toPE2 family l2vpn signaling
set protocols bgp group toPE2 neighbor 10.255.7.7
set protocols ospf area 0.0.0.0 interface ge-2/0/2.0
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ldp interface ge-2/0/2.0
set protocols ldp interface lo0.0
set routing-instances titanium instance-type vpls
set routing-instances titanium vlan-id none
set routing-instances titanium interface ge-2/0/0.0
set routing-instances titanium interface ge-2/0/1.0
set routing-instances titanium route-distinguisher 101:101
set routing-instances titanium vrf-target target:201:201
set routing-instances titanium protocols vpls vpls-id 15
set routing-instances titanium protocols vpls site pe1 site-identifier 1
set routing-instances titanium protocols pim-snooping
```

Router CE1

```
set interfaces ge-2/0/0 unit 0 description toPE1
set interfaces ge-2/0/0 unit 0 family inet address 10.0.0.10/30
set interfaces lo0 unit 0 family inet address 10.255.2.2./32
set routing-options router-id 10.255.2.2
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols pim rp static address 10.255.3.3
set protocols pim interface all
```

Router CE2

```
set interfaces ge-2/0/0 unit 0 description toPE1
set interfaces ge-2/0/0 unit 0 family inet address 10.0.0.6/30
set interfaces ge-2/0/1 unit 0 description toReceiver1
set interfaces ge-2/0/1 unit 0 family inet address 10.0.0.13/30
set interfaces lo0 unit 0 family inet address 10.255.2.2
set routing-options router-id 10.255.2.2
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols pim rp static address 10.255.3.3
set protocols pim interface all
```

Router PE2

```
set multicast-snooping-options traceoptions file snoop.log size 10m
set interfaces ge-2/0/0 encapsulation ethernet-vpls
set interfaces ge-2/0/0 unit 0 description toCE3
set interfaces ge-2/0/1 encapsulation ethernet-vpls
set interfaces ge-2/0/1 unit 0 description toCE4
set interfaces ge-2/0/2 unit 0 description toPE1
set interfaces ge-2/0/2 unit 0 family inet address 10.0.0.2/30
set interfaces ge-2/0/2 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 10.255.7.7/32
set routing-options router-id 10.255.7.7
set protocols mpls interface ge-2/0/2.0
set protocols bgp group toPE1 type internal
set protocols bgp group toPE1 local-address 10.255.7.7
set protocols bgp group toPE1 family l2vpn signaling
set protocols bgp group toPE1 neighbor 10.255.1.1
set protocols ospf area 0.0.0.0 interface ge-2/0/2.0
```

```

set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ldp interface ge-2/0/2.0
set protocols ldp interface lo0.0
set routing-instances titanium instance-type vpls
set routing-instances titanium vlan-id none
set routing-instances titanium interface ge-2/0/0.0
set routing-instances titanium interface ge-2/0/1.0
set routing-instances titanium route-distinguisher 101:101
set routing-instances titanium vrf-target target:201:201
set routing-instances titanium protocols vpls vpls-id 15
set routing-instances titanium protocols vpls site pe2 site-identifier 2
set routing-instances titanium protocols pim-snooping

```

Router CE3 (RP)

```

set interfaces ge-2/0/0 unit 0 description toPE2
set interfaces ge-2/0/0 unit 0 family inet address 10.0.0.18/30
set interfaces ge-2/0/1 unit 0 description toSource
set interfaces ge-2/0/1 unit 0 family inet address 10.0.0.29/30
set interfaces lo0 unit 0 family inet address 10.255.3.3/32
set routing-options router-id 10.255.3.3
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols pim rp local address 10.255.3.3
set protocols pim interface all

```

Router CE4

```

set interfaces ge-2/0/0 unit 0 description toPE2
set interfaces ge-2/0/0 unit 0 family inet address 10.0.0.22/30
set interfaces ge-2/0/1 unit 0 description toReceiver2
set interfaces ge-2/0/1 unit 0 family inet address 10.0.0.25/30
set interfaces lo0 unit 0 family inet address 10.255.4.4/32
set routing-options router-id 10.255.4.4
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols pim rp static address 10.255.3.3
set protocols pim interface all

```

Configuring PIM Snooping for VPLS

Step-by-Step Procedure The following example requires that you navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.



NOTE: This section includes a step-by-step configuration procedure for one or more routers in the topology. For comprehensive configurations for all routers, see “[CLI Quick Configuration](#)” on page 161.

To configure PIM snooping for VPLS:

1. Configure the router interfaces forming the links between the routers.

Router PE2

[edit interfaces]

user@PE2# set ge-2/0/0 encapsulation ethernet-vpls

```

user@PE2# set ge-2/0/0 unit 0 description toCE3
user@PE2# set ge-2/0/1 encapsulation ethernet-vpls
user@PE2# set ge-2/0/1 unit 0 description toCE4
user@PE2# set ge-2/0/2 unit 0 description toPE1
user@PE2# set ge-2/0/2 unit 0 family mpls
user@PE2# set ge-2/0/2 unit 0 family inet address 10.0.0.2/30
user@PE2# set lo0 unit 0 family inet address 10.255.7.7/32

```



NOTE: ge-2/0/0.0 and ge-2/0/1.0 are configured as VPLS interfaces and connect to Routers CE3 and CE4. See *Virtual Private LAN Service Feature Guide* for more details.

Router CE3

[edit interfaces]

```

user@CE3# set ge-2/0/0 unit 0 description toPE2
user@CE3# set ge-2/0/0 unit 0 family inet address 10.0.0.18/30
user@CE3# set ge-2/0/1 unit 0 description toSource
user@CE3# set ge-2/0/1 unit 0 family inet address 10.0.0.29/30
user@CE3# set lo0 unit 0 family inet address 10.255.3.3/32

```



NOTE: The ge-2/0/1.0 interface on Router CE3 connects to the multicast source.

Router CE4

[edit interfaces]

```

user@CE4# set ge-2/0/0 unit 0 description toPE2
user@CE4# set ge-2/0/0 unit 0 family inet address 10.0.0.22/30
user@CE4# set ge-2/0/1 unit 0 description toReceiver2
user@CE4# set ge-2/0/1 unit 0 family inet address 10.0.0.25/30
user@CE4# set lo0 unit 0 family inet address 10.255.4.4/32

```



NOTE: The ge-2/0/1.0 interface on Router CE4 connects to a multicast receiver.

Similarly, configure Routers PE1, CE1, and CE2.

2. Configure the router IDs of all routers.

Router PE2

[edit routing-options]

```
user@PE2# set router-id 10.255.7.7
```

Similarly, configure other routers.

3. Configure an IGP on interfaces of all routers.

Router PE2

[edit protocols ospf area 0.0.0.0]

```
user@PE2# set interface ge-2/0/2.0
```

```
user@PE2# set interface lo0.0
```

Similarly, configure other routers.

4. Configure the LDP, MPLS, and BGP protocols on the PE routers.

```
Router PE2
[edit protocols]
user@PE2# set ldp interface lo0.0
user@PE2# set mpls interface ge-2/0/2.0
user@PE2# set bgp group toPE1 type internal
user@PE2# set bgp group toPE1 local-address 10.255.7.7
user@PE2# set bgp group toPE1 family l2vpn signaling
user@PE2# set bgp group toPE1 neighbor 10.255.1.1
user@PE2# set ldp interface ge-2/0/2.0
```

The BGP group is required for interfacing with the other PE router. Similarly, configure Router PE1.

5. Configure PIM on all CE routers.

Ensure that Router CE3 is configured as the rendezvous point (RP) and that the RP address is configured on other CE routers.

```
Router CE3
[edit protocols pim]
user@CE3# set rp local address 10.255.3.3
user@CE3# set interface all
```

```
Router CE4
[edit protocols pim]
user@CE4# set rp static address 10.255.3.3
user@CE4# set interface all
```

Similarly, configure Routers CE1 and CE2.

6. Configure multicast snooping options on the PE routers.

```
Router PE2
[edit multicast-snooping-options traceoptions]
user@PE2# set file snoop.log size 10m
```

Similarly, configure Router PE1.

7. Create a routing instance (**titanium**), and configure the VPLS on the PE routers.

```
Router PE2
[edit routing-instances titanium]
user@PE2# set instance-type vpls
user@PE2# set vlan-id none
user@PE2# set interface ge-2/0/0.0
user@PE2# set interface ge-2/0/1.0
user@PE2# set route-distinguisher 101:101
user@PE2# set vrf-target target:201:201
user@PE2# set protocols vpls vpls-id 15
user@PE2# set protocols vpls site pe2 site-identifier 2
```

Similarly, configure Router PE1.

8. Configure PIM snooping on the PE routers.

```
Router PE2
```

```
[edit routing-instances titanium]
user@PE2# set protocols pim-snooping
```

Similarly, configure Router PE1.

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show routing-options**, **show protocols**, **show multicast-snooping-options**, and **show routing-instances** commands.

If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@PE2# show interfaces
ge-2/0/2 {
  unit 0 {
    description toPE1
    family inet {
      address 10.0.0.2/30;
    }
    family mpls;
  }
}
ge-2/0/0 {
  encapsulation ethernet-vpls;
  unit 0 {
    description toCE3;
  }
}
ge-2/0/1 {
  encapsulation ethernet-vpls;
  unit 0 {
    description toCE4;
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.255.7.7/32;
    }
  }
}
```

```
user@PE2# show routing-options
router-id 10.255.7.7;
```

```
user@PE2# show protocols
mpls {
  interface ge-2/0/2.0;
}
ospf {
  area 0.0.0.0 {
    interface ge-2/0/2.0;
    interface lo0.0;
  }
}
ldp {
  interface ge-2/0/2.0;
```



```

        interface lo0.0;
    }
    bgp {
        group toPE1 {
            type internal;
            local-address 10.255.7.7;
            family l2vpn {
                signaling;
            }
            neighbor 10.255.1.1;
        }
    }

user@PE2# show multicast-snooping-options
traceoptions {
    file snoop.log size 10m;
}

user@PE2# show routing-instances
titanium {
    instance-type vpls;
    vlan-id none;
    interface ge-2/0/0.0;
    interface ge-2/0/1.0;
    route-distinguisher 101:101;
    vrf-target target:201:201;
    protocols {
        vpls {
            site pe2 {
                site-identifier 2;
            }
            vpls-id 15;
        }
        pim-snooping;
    }
}

```

Similarly, confirm the configuration on all other routers. If you are done configuring the routers, enter **commit** from configuration mode.



NOTE: Use the **show protocols** command on the CE routers to verify the configuration for the PIM RP.

Verification

Confirm that the configuration is working properly.

- [Verifying PIM Snooping for VPLS on page 167](#)

Verifying PIM Snooping for VPLS

Purpose Verify that PIM Snooping is operational in the network.

Action To verify that PIM snooping is working as desired, use the following commands:

- *show pim snooping interfaces*
- *show pim snooping neighbors detail*
- *show pim snooping statistics*
- *show pim snooping join*
- *show pim snooping join extensive*
- *show multicast snooping route* extensive instance *<instance-name>* group *<group-name>*

1. From operational mode on Router PE2, run the **show pim snooping interfaces** command.

```
user@PE2> show pim snooping interfaces
Instance: titanium
```

```
Learning-Domain: default
```

Name	State	IP	NbrCnt
ge-2/0/0.0	Up	4	1
ge-2/0/1.0	Up	4	1

```
DR address: 10.0.0.22
DR flooding is ON
```

The output verifies that PIM snooping is configured on the two interfaces connecting Router PE2 to Routers CE3 and CE4.

Similarly, check the PIM snooping interfaces on Router PE1.

2. From operational mode on Router PE2, run the **show pim snooping neighbors detail** command.

```
user@PE2> show pim snooping neighbors detail
Instance: titanium
Learning-Domain: default
```

```
Interface: ge-2/0/0.0
```

```
Address: 10.0.0.18
Uptime: 00:17:06
Hello Option Holdtime: 105 seconds 99 remaining
Hello Option DR Priority: 1
Hello Option Generation ID: 552495559
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
                             Tracking is supported
```

```
Interface: ge-2/0/1.0
```

```
Address: 10.0.0.22
Uptime: 00:15:16
Hello Option Holdtime: 105 seconds 103 remaining
Hello Option DR Priority: 1
Hello Option Generation ID: 1131703485
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
                             Tracking is supported
```

The output verifies that Router PE2 can detect the IP addresses of its PIM snooping neighbors (10.0.0.18 on CE3 and 10.0.0.22 on CE4).

Similarly, check the PIM snooping neighbors on Router PE1.

3. From operational mode on Router PE2, run the **show pim snooping statistics** command.

```
user@PE2> show pim snooping statistics
Instance: titanium
```

```
Learning-Domain: default
```

Tx J/P messages	0
Rx J/P messages	246
Rx J/P messages -- seen	0
Rx J/P messages -- received	246
Rx Hello messages	1036
Rx Version Unknown	0
Rx Neighbor Unknown	0
Rx Upstream Neighbor Unknown	0
Rx J/P Busy Drop	0
Rx J/P Group Aggregate	0
Rx Malformed Packet	0
Rx No PIM Interface	0
Rx Bad Length	0
Rx Unknown Hello Option	0
Rx Unknown Packet Type	0
Rx Bad TTL	0
Rx Bad Destination Address	0
Rx Bad Checksum	0
Rx Unknown Version	0

The output shows the number of hello and join/prune messages received by Router PE2. This verifies that PIM sparse mode is operational in the network.

4. Send multicast traffic from the source terminal attached to Router CE3, for the multicast group 224.1.1.1.
5. From operational mode on Router PE2, run the **show pim snooping join**, **show pim snooping join extensive**, and **show multicast snooping route extensive instance <instance-name> group <group-name>** commands to verify PIM snooping.

```
user@PE2> show pim snooping join
```

```
Instance: titanium
Learning-Domain: default
```

```
Group: 224.1.1.1
Source: *
Flags: sparse,rptree,wildcard
Upstream neighbor: 10.0.0.18, Port: ge-2/0/0.0
```

```
Group: 224.1.1.1
Source: 10.0.0.30
Flags: sparse
Upstream neighbor: 10.0.0.18, Port: ge-2/0/0.0
```

```
user@PE2> show pim snooping join extensive
```

```
Instance: titanium
Learning-Domain: default
```

```
Group: 224.1.1.1
Source: *
Flags: sparse,rptree,wildcard
Upstream neighbor: 10.0.0.18, Port: ge-2/0/0.0
Downstream port: ge-2/0/1.0
Downstream neighbors:
10.0.0.22 State: Join Flags: SRW Timeout: 180
```

```
Group: 224.1.1.1
Source: 10.0.0.30
Flags: sparse
Upstream neighbor: 10.0.0.18, Port: ge-2/0/0.0
Downstream port: ge-2/0/1.0
Downstream neighbors:
10.0.0.22 State: Join Flags: S Timeout: 180
```

The outputs show that multicast traffic sent for the group 224.1.1.1 is sent to Receiver 2 through Router CE4 and also display the upstream and downstream neighbor details.

```
user@PE2> show multicast snooping route extensive instance titanium group 224.1.1.1
Nexthop Bulking: OFF
```

```
Family: INET
```

```
Group: 224.1.1.1/32
Bridge-domain: titanium
Mesh-group: __all_ces__
Downstream interface list:
ge-2/0/1.0 -(1072)
Statistics: 0 kbps, 0 pps, 0 packets
Next-hop ID: 1048577
Route state: Active
Forwarding state: Forwarding
```

```
Group: 224.1.1.1/32
Source: 10.0.0.8
Bridge-domain: titanium
Mesh-group: __all_ces__
Downstream interface list:
ge-2/0/1.0 -(1072)
Statistics: 0 kbps, 0 pps, 0 packets
Next-hop ID: 1048577
Route state: Active
Forwarding state: Forwarding
```

Meaning PIM snooping is operational in the network.

PART 7

Configuration Statements and Operational Commands

- Configuration Statements: IGMP on page 173
- Configuration Statements: IGMP Snooping on page 201
- Configuration Statements: MLD on page 221
- Configuration Statements: MLD Snooping on page 243
- Configuration Statements: MSDP on page 261
- Configuration Statements: PIM on page 287
- Operational Commands: IGMP on page 399
- Operational Commands: IGMP Snooping on page 413
- Operational Commands: MLD on page 431
- Operational Commands: MLD Snooping on page 447
- Operational Commands: MSDP on page 475
- Operational Commands: PIM on page 505

CHAPTER 12

Configuration Statements: IGMP

- [igmp](#) on page 175
- [accounting \(Protocols IGMP Interface\)](#) on page 176
- [accounting \(Protocols IGMP\)](#) on page 176
- [disable \(Protocols IGMP\)](#) on page 177
- [exclude \(Protocols IGMP\)](#) on page 177
- [group \(Protocols IGMP\)](#) on page 178
- [group-count \(Protocols IGMP\)](#) on page 179
- [group-increment \(Protocols IGMP\)](#) on page 179
- [group-limit \(IGMP\)](#) on page 180
- [group-policy \(Protocols IGMP\)](#) on page 181
- [group-threshold \(Protocols IGMP Interface\)](#) on page 182
- [immediate-leave \(Protocols IGMP\)](#) on page 183
- [interface \(Protocols IGMP\)](#) on page 184
- [log-interval \(Protocols IGMP Interface\)](#) on page 185
- [maximum-transmit-rate \(Protocols IGMP\)](#) on page 186
- [oif-map \(IGMP Interface\)](#) on page 186
- [passive \(IGMP\)](#) on page 187
- [promiscuous-mode \(Protocols IGMP\)](#) on page 188
- [query-interval \(Protocols IGMP\)](#) on page 189
- [query-last-member-interval \(Protocols IGMP\)](#) on page 190
- [query-response-interval \(Protocols IGMP\)](#) on page 191
- [robust-count \(Protocols IGMP\)](#) on page 192
- [source \(Protocols IGMP\)](#) on page 193
- [source-count \(Protocols IGMP\)](#) on page 194
- [source-increment \(Protocols IGMP\)](#) on page 195
- [ssm-map \(Protocols IGMP\)](#) on page 195
- [ssm-map-policy \(IGMP\)](#) on page 196
- [static \(Protocols IGMP\)](#) on page 197

- [traceoptions \(Protocols IGMP\) on page 198](#)
- [version \(Protocols IGMP\) on page 200](#)

igmp

```
Syntax  igmp {
    accounting;
    interface interface-name {
        disable;
        (accounting | no-accounting);
        group-limit limit;
        group-policy [ policy-names ];
        group-threshold
        immediate-leave;
        log-interval
        oif-map map-name;
        passive;
        promiscuous-mode;
        ssm-map ssm-map-name;
        ssm-map-policy ssm-map-policy-name;
        static {
            group multicast-group-address {
                exclude;
                group-count number;
                group-increment increment;
                source ip-address {
                    source-count number;
                    source-increment increment;
                }
            }
        }
        version version;
    }
    query-interval seconds;
    query-last-member-interval seconds;
    query-response-interval seconds;
    robust-count number;
    traceoptions {
        file filename <files number> <size size> <world-readable | no-world-readable>;
        flag flag <flag-modifier> <disable>;
    }
}
```

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

Release Information Statement introduced before Junos OS Release 7.4.
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.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Enable IGMP on the router or switch. IGMP must be enabled for the router or switch to receive multicast packets.

The remaining statements are explained separately.

Default	IGMP is disabled on the router or switch. IGMP is automatically enabled on all broadcast interfaces when you configure Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP).
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Enabling IGMP on page 24

accounting (Protocols IGMP Interface)

Syntax	(accounting no-accounting);
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 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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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">• Recording IGMP Join and Leave Events on page 37

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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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">• Recording IGMP Join and Leave Events on page 37


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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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"> • Disabling IGMP on page 42

exclude (Protocols IGMP)

Syntax	exclude;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i> static group <i>mcast-group-address</i>], [edit protocols igmp interface <i>interface-name</i> static group <i>mcast-group-address</i>]
Release Information	Statement introduced in Junos OS Release 9.3. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the static group to operate in exclude mode. In exclude mode all sources except the address configured are accepted for the group. If this statement is not included, the group operates in include mode.
Required Privilege Level	view-level—To view this statement in the configuration. control-level—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Enabling IGMP Static Group Membership on page 31

group (Protocols IGMP)

Syntax	<pre>group <i>multicast-group-address</i> { <i>exclude</i>; <i>group-count number</i>; <i>group-increment increment</i>; source <i>ip-address</i> { <i>source-count number</i>; <i>source-increment increment</i>; } }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols <i>igmp interface interface-name static</i>], [edit protocols <i>igmp interface interface-name static</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 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">• Enabling IGMP Static Group Membership on page 31

group-count (Protocols IGMP)

Syntax	<code>group-count <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i> static group <i>mcast-group-address</i>], [edit protocols igmp interface <i>interface-name</i> static group <i>mcast-group-address</i>]
Release Information	Statement introduced in Junos OS Release 9.6. 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 number of static groups to be created.
Options	<i>number</i> —Number of static groups. Range: 1 through 512
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Enabling IGMP Static Group Membership on page 31

group-increment (Protocols IGMP)

Syntax	<code>group-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>mcast-group-address</i>], [edit protocols igmp interface <i>interface-name</i> static group <i>mcast-group-address</i>]
Release Information	Statement introduced in Junos OS Release 9.6. 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	Configure the number of times the address should be incremented for each static group created. The increment is specified in dotted decimal notation similar to an IPv4 address.
Options	<i>increment</i> —Number of times the address should be incremented. Default: 0.0.0.1 Range: 0.0.0.1 through 255.255.255.255
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Enabling IGMP Static Group Membership on page 31

group-limit (IGMP)

Syntax	<code>group-limit <i>limit</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 10.4. 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	<p>Configure a limit for the number of multicast groups (or [S,G] channels in IGMPv3) allowed on an interface. After this limit is reached, new reports are ignored and all related flows are not flooded on the interface.</p> <p>To confirm the configured group limit on the interface, use the show igmp interface command.</p>
Default	By default, there is no limit to the number of multicast groups that can join the interface.
Options	<i>limit</i> —group limit value for the interface. Range: 1 through 32767
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">• Limiting the Number of IGMP Multicast Group Joins on Logical Interfaces on page 39• group-threshold on page 182• log-interval on page 185


group-policy (Protocols IGMP)

Syntax	<code>group-policy [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.1. 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	When this statement is enabled on a router running IGMP version 2 (IGMPv2) or version 3 (IGMPv3), after the router receives an IGMP report, the router compares the group against the specified group policy and performs the action configured in that policy (for example, rejects the report).
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Filtering Unwanted IGMP Reports at the IGMP Interface Level on page 27

group-threshold (Protocols IGMP Interface)

Syntax	<code>group-threshold value;</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 12.2.
Description	<p>Specify the threshold at which a warning message is logged for the multicast groups received on a logical interface. The threshold is a percentage of the maximum number of multicast groups allowed on a logical interface.</p> <p>For example, if you configure a maximum number of 1,000 incoming multicast groups, and you configure a threshold value of 90 percent, warning messages are logged in the system log when the interface receives 900 groups.</p> <p>To confirm the configured group threshold on the interface, use the show igmp interface command.</p>
Default	By default, there is no configured threshold value.
Options	<p>value—Percentage of the maximum number of multicast groups allowed on the interface that starts triggering the warning. You configure a percentage of the group-limit value that starts triggering the warnings. You must explicitly configure the group-limit to configure a threshold value.</p> <p>Range: 1 through 100</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">• Limiting the Number of IGMP Multicast Group Joins on Logical Interfaces on page 39• group-limit on page 180• log-interval on page 185

immediate-leave (Protocols IGMP)

Syntax	<code>immediate-leave;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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>Starting in Junos OS Release 9.3, both IGMP version 2 and IGMP version 3 do host tracking when the immediate-leave statement is configured. This means that the multicast group leaves only when the last host leaves. The routing 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 routing device 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**
- [Specifying Immediate-Leave Host Removal for IGMP on page 26](#)

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	<p>[edit logical-systems <i>logical-system-name</i> protocols igmp],</p> <p>[edit protocols igmp]</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 12.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Enable IGMP on an interface and configure interface-specific properties.</p>
Options	<p><i>interface-name</i>—Name of the interface. Specify the full interface name, including the physical and logical address components. To configure all interfaces, you can specify all.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Enabling IGMP on page 24

log-interval (Protocols IGMP Interface)

Syntax	log-interval <i>seconds</i> ;
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 12.2.
Description	<p>Specify the minimum time interval (in seconds) between sending consecutive log messages to the system log for multicast groups. To configure the time interval, you must specify the maximum number of multicast groups allowed on the interface. You must configure the group-limit statement before you configure the log-interval statement.</p> <p>To confirm the configured log interval on the interface, use the show igmp interface command.</p>
Default	By default, there is no configured time interval.
Options	<p>seconds—Minimum time interval (in seconds) between log messages. You must explicitly configure the group-limit to configure a time interval to send log messages.</p> <p>Range: 6 through 32,767 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"> • Limiting the Number of IGMP Multicast Group Joins on Logical Interfaces on page 39 • group-limit on page 180 • group-threshold on page 182


maximum-transmit-rate (Protocols IGMP)

Syntax	<code>maximum-transmit-rate <i>packets-per-second</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp], [edit protocols igmp]
Release Information	Statement introduced in Junos OS Release 9.3. 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	Limit the transmission rate of IGMP packets
Options	packets-per-second —Maximum number of IGMP packets transmitted in one second by the routing device. Range: 1 through 10000 Default: 500 packets
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">• Limiting the Maximum IGMP Message Rate on page 30

oif-map (IGMP Interface)

Syntax	<code>oif-map <i>map-name</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6. 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	Associates an outgoing interface (OIF) map to the IGMP interface. The OIF map is a routing policy statement that can contain multiple terms.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Multicast with Subscriber VLANs

passive (IGMP)

Syntax	<code>passive <allow-receive> <send-general-query> <send-group-query>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6. allow-receive , send-general-query , and send-group-query options were added in Junos OS Release 10.0. 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 that IGMP run on the interface and either not send and receive control traffic or selectively send and receive control traffic such as IGMP reports, queries, and leaves.
<div>  <p>NOTE: You can selectively activate up to two out of the three available options for the passive statement while keeping the other functions passive (inactive). Activating all three options would be equivalent to not using the passive statement.</p> </div>	
Options	<p>allow-receive—Enables IGMP to receive control traffic on the interface.</p> <p>send-general-query—Enables IGMP to send general queries on the interface.</p> <p>send-group-query—Enables IGMP to send group-specific and group-source-specific queries on the interface.</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 Multicast with Subscriber VLANs</i> • Enabling IGMP on page 24

promiscuous-mode (Protocols IGMP)

Syntax	<code>promiscuous-mode;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>], [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 9.2 for dynamic profiles. 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 that the interface accepts IGMP reports from hosts on any subnetwork. Note that when enabling promiscuous-mode, all routing devices on the ethernet segment must be configured with the promiscuous mode statement. Otherwise, only the interface configured with lowest IPv4 address acts as the querier for IGMP for this Ethernet segment.
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>Dynamic IGMP Configuration Overview</i>• <i>Configuring Dynamic DHCP Client Access to a Multicast Network</i>• Accepting IGMP Messages from Remote Subnetworks on page 28

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"> • Modifying the IGMP Host-Query Message Interval on page 25 • query-last-member-interval (Protocols IGMP) on page 190 • query-response-interval (Protocols IGMP) on page 191

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 999999 Default: 1 second
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Modifying the IGMP Last-Member Query Interval on page 29• query-interval (Protocols IGMP) on page 189• query-response-interval (Protocols IGMP) on page 191

query-response-interval (Protocols IGMP)

Syntax	<code>query-response-interval <i>seconds</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp], [edit protocols igmp]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. 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	<i>seconds</i> —The query response interval must be less than the query interval. Range: 1 through 1024 Default: 10 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Modifying the IGMP Query Response Interval on page 26 • query-interval (Protocols IGMP) on page 189 • query-last-member-interval (Protocols IGMP) on page 190

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">• Modifying the IGMP Robustness Variable on page 29

source (Protocols IGMP)

Syntax	<pre>source <i>ip-address</i> { <i>source-count</i> <i>number</i>; <i>source-increment</i> <i>increment</i>; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i> static group <i>mcast-group-address</i>], [edit protocols igmp interface <i>interface-name</i> static group <i>mcast-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	<p><i>ip-address</i>—IPv4 unicast address.</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"> • Enabling IGMP Static Group Membership on page 31

source-count (Protocols IGMP)

Syntax	<code>source-count <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i> static group multicast-group-address source], [edit protocols igmp interface <i>interface-name</i> static group multicast-group-address source]
Release Information	Statement introduced in Junos OS Release 9.6. 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	Configure the number of multicast source addresses that should be accepted for each static group created.
Options	<i>number</i> —Number of source addresses. Default: 1 Range: 1 through 1024
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Enabling IGMP Static Group Membership on page 31

source-increment (Protocols IGMP)

Syntax	<code>source-increment <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i> static group <i>mcast-group-address</i> source], [edit protocols igmp interface <i>interface-name</i> static group <i>mcast-group-address</i> source]
Release Information	Statement introduced in Junos OS Release 9.6. 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	Configure the number of times the multicast source address should be incremented for each static group created. The increment is specified in dotted decimal notation similar to an IPv4 address.
Options	increment —Number of times the source address should be incremented. Default: 0.0.0.1 Range: 0.0.0.1 through 255.255.255.255
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Enabling IGMP Static Group Membership on page 31

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

ssm-map-policy (IGMP)

Syntax	<code>ssm-map-policy <i>ssm-map-policy-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 11.4. 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 policy to an IGMP interface.
Options	<i>ssm-map-policy-name</i> —Name of SSM map policy.
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 Maps for Different Groups to Different Sources</i>

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 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

- [Enabling IGMP Static Group Membership on page 31](#)

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	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	<p>Configure IGMP tracing options.</p> <p>To specify more than one tracing operation, include multiple flag statements.</p> <p>To trace the paths of multicast packets, use the mtrace command.</p>
Default	The default IGMP trace options are those inherited from the routing protocols traceoptions statement included at the [edit routing-options] hierarchy level.
Options	<p>disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.</p> <p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. We recommend that you place tracing output in the file igmp-log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you must also include the size statement to specify the maximum file size.</p> <p>Range: 2 through 1000 files</p> <p>Default: 2 files</p> <p>flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.</p> <p>IGMP Tracing Flags</p> <ul style="list-style-type: none">• leave—Leave group messages (for IGMP version 2 only).• mtrace—Mtrace packets. Use the mtrace command to troubleshoot the software.

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

Global Tracing Flags

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

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

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

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

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

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

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

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

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

Default: If you do not include this option, tracing output is appended to an existing trace file.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When **trace-file** again reaches this size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

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

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

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

Default: 1 MB

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

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

Related Documentation

- [Tracing IGMP Protocol Traffic on page 40](#)

version (Protocols IGMP)

Syntax `version version;`

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 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

- [Changing the IGMP Version on page 31](#)

CHAPTER 13

Configuration Statements: IGMP Snooping

- [igmp-snooping](#) on page 202
- [group](#) (Bridge Domains) on page 203
- [group-limit](#) (IGMP and MLD Snooping) on page 204
- [host-only-interface](#) on page 205
- [immediate-leave](#) (Bridge Domains) on page 206
- [interface](#) (Bridge Domains) on page 208
- [multicast-router-interface](#) (IGMP Snooping) on page 209
- [proxy](#) (Bridge Domains) on page 210
- [query-interval](#) (Bridge Domains) on page 211
- [query-last-member-interval](#) (Bridge Domains) on page 212
- [query-response-interval](#) (Bridge Domains) on page 213
- [robust-count](#) (Bridge Domains) on page 214
- [source](#) (Bridge Domains) on page 215
- [source-address](#) on page 215
- [static](#) (Bridge Domains) on page 216
- [traceoptions](#) (Protocols IGMP Snooping) on page 217
- [vlan](#) (Bridge Domains) on page 219

igmp-snooping

```
Syntax  igmp-snooping {
        vlan vlan-id {
            immediate-leave;
            interface interface-name {
                group-limit limit;
                host-only-interface;
                immediate-leave;
                multicast-router-interface;
                static {
                    group ip-address {
                        source ip-address;
                    }
                }
            }
        }
        proxy {
            source-address ip-address;
        }
        query-interval seconds;
        query-last-member-interval seconds;
        query-response-interval seconds;
        robust-count number;
    }
```

Hierarchy Level [edit protocols]

Release Information Statement introduced in Junos OS Release 8.5.

Description Enable IGMP snooping on the router or switch.

Default IGMP snooping is disabled on the router or switch.

Options The 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

- *Understanding IGMP Snooping*
- *IGMP Snooping in MC-LAG Active-Active Mode on MX Series Routers Overview*

group (Bridge Domains)

Syntax	<code>group <i>ip-address</i> { <i>source-address</i> <i>ip-address</i>; }</code>
Hierarchy Level	[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>interface</i> <i>interface-name</i> <i>static</i>], [edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>vlan</i> <i>vlan-id</i> <i>interface</i> <i>interface-name</i> <i>static</i>], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>interface</i> <i>interface-name</i> <i>static</i>], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols <i>vlan</i> <i>vlan-id</i> igmp-snooping <i>interface</i> <i>interface-name</i> <i>static</i>]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Configure the IGMP multicast group address that receives data on an interface and (optionally) a source address for certain packets.
Options	<i>ip-address</i> —Group address. The remaining statement is 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>Example: Configuring IGMP Snooping</i>

group-limit (IGMP and MLD Snooping)

Syntax	<code>group-limit <i>limit</i>;</code>
Hierarchy Level	<code>[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>interface</i> <i>interface-name</i>]</code> <code>[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>vlan</i> <i>vlan-id</i> <i>interface</i> <i>interface-name</i>]</code> <code>[edit bridge-domains <i>bridge-domain-name</i> protocols mld-snooping <i>interface</i> <i>interface-name</i>]</code> <code>[edit bridge-domains <i>bridge-domain-name</i> protocols mld-snooping <i>vlan</i> <i>mld-snooping-vlan</i> <i>interface</i> <i>interface-name</i>]</code> <code>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>interface</i> <i>interface-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols <i>vlan</i> <i>vlan-id</i> igmp-snooping <i>interface</i> <i>interface-name</i>]</code> <code>[edit protocols igmp-snooping <i>vlan</i> <i>interface</i>]</code>
Release Information	Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 13.2 for the QFX series.
Description	Configure a limit for the number of multicast groups (or [S,G] channels in IGMPv3) allowed on an interface. After this limit is reached, new reports are ignored and all related flows are not flooded on the interface.
Default	By default, there is no limit to the number of multicast groups joining an interface.
Options	<i>limit</i> —a 32-bit number for the limit on the interface. Range: 1 through 32,767. For MX series routers, the range is 1 to 65535. Starting with Junos OS release 14.2, a value of 0, which was treated as null, is not supported.
Required Privilege Level	<i>routing</i> —To view this statement in the configuration. <i>routing-control</i> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring IGMP Snooping</i>

host-only-interface

Syntax	host-only-interface;
Hierarchy Level	<p>[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface interface-name],</p> <p>[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping vlan vlan-id interface interface-name],</p> <p>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface interface-name],</p> <p>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols vlan vlan-id igmp-snooping interface interface-name]</p> <p>[edit protocols igmp-snooping vlan interface]</p> <p>[edit protocols mld-snooping vlan vlan-id interface <i>interface-name</i>]</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols mld-snooping vlan vlan-id 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 13.2 for the QFX series.</p> <p>Support at the [edit protocols mld-snooping vlan vlan-id interface interface-name] and the [edit routing-instances <i>routing-instance-name</i> protocols mld-snooping vlan vlan-id interface interface-name] hierarchy levels introduced in Junos OS Release 13.3 for EX Series switches.</p>
Description	Configure an interface as a host-facing interface. IGMP and MLD queries received on these interfaces are dropped.
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"> • Example: Configuring IGMP Snooping • multicast-router-interface on page 209

immediate-leave (Bridge Domains)

Syntax	<code>immediate-leave;</code>
Hierarchy Level	<pre> [edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping], [edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>interface</i> <i>interface-name</i>], [edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>vlan</i> <i>vlan-id</i> <i>interface</i> <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>interface</i> <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols <i>vlan</i> <i>vlan-id</i> igmp-snooping <i>interface</i> <i>interface-name</i>] [edit protocols igmp-snooping <i>vlan</i> <i>interface</i>] [edit bridge-domains <i>bridge-domain-name</i> protocols mld-snooping], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols mld-snooping] [edit routing-instances <i>routing-instance-name</i> protocols mld-snooping] </pre>
Release Information	<p>Statement introduced in Junos OS Release 8.5.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX series.</p> <p>Statement introduced in Junos OS Release 14.2 for MX series Routers with MPC.</p>
Description	<p>The immediate leave setting is useful for minimizing the leave latency of IGMP or MLD (for IPv6) 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 or MLD 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 or MLD group-specific queries to the interface. The interface is pruned from the multicast tree for the multicast group specified in the 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>



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 routing device only knows about the one interested host and does not know about the others.

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

Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring IGMP Snooping</i>
------------------------------	---

interface (Bridge Domains)

Syntax	<pre> interface <i>interface-name</i> { <i>group-limit limit</i>; <i>host-only-interface</i>; <i>multicast-router-interface</i>; static { <i>group ip-address</i> { <i>source ip-address</i>; } } } </pre>
Hierarchy Level	<pre> [edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping], [edit bridge-domains <i>bridge-domain-name</i> protocols mld-snooping], [edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>vlan vlan-id</i>], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols mld-snooping], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols <i>vlan vlan-id</i> igmp-snooping] [edit routing-instances <i>routing-instance-name</i> protocols mld-snooping] [edit protocols igmp-snooping <i>vlan</i>], </pre>
Release Information	<p>Statement introduced in Junos OS Release 8.5.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX series.</p> <p>Statement introduced in Junos OS Release 14.2 for MX series Routers with MPC.</p>
Description	Enable IGMP or MLD snooping 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>Example: Configuring IGMP Snooping</i> • <i>mld-snooping</i> • <i>igmp-snooping</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	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.



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.

Configure an interface as a bridge interface toward other multicast routing devices.

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 on MX Series Routers Overview</i> • host-only-interface on page 205

proxy (Bridge Domains)

Syntax	<pre>proxy { source-address ip-address; }</pre>
Hierarchy Level	<pre>[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping], [edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>vlan</i> <i>vlan-id</i>], [edit bridge-domains <i>bridge-domain-name</i> protocols mld-snooping], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols mld-snooping], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols <i>vlan</i> <i>vlan-id</i> igmp-snooping] [edit routing-instances <i>routing-instance-name</i> protocols mld-snooping]</pre>
Release Information	Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 14.2 for MX series Routers with MPC.
Description	Configure proxy mode and options, including source address. All the queries generated by IGMP snooping are sent using 0.0.0.0 as the source address in order to avoid participating in IGMP querier election. Also, all reports generated by IGMP snooping are sent with 0.0.0.0 as the source address unless there is a configured source address to use.
Default	By default, IGMP and MLD snooping do not employ proxy mode. The remaining statement is 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>Example: Configuring MLD Snooping</i>• <i>Examples: Configuring MLD</i>• <i>mld-snooping</i>

query-interval (Bridge Domains)

Syntax	<code>query-interval seconds;</code>
Hierarchy Level	<pre>[edit bridge-domains <i>bridge-domain-name</i> protocols mld-snooping] , [edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>interface</i> <i>interface-name</i>], [edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>vlan</i> <i>vlan-id</i> <i>interface</i> <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>interface</i> <i>interface-name</i>],[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols mld-snooping] [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping <i>vlan</i> <i>vlan-id</i> <i>interface</i> <i>interface-name</i>] [edit routing-instances <i>routing-instance-name</i> protocols mld-snooping] [edit protocols igmp-snooping <i>vlan</i>]</pre>
Release Information	<p>Statement introduced before Junos OS Release 8.5.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX series.</p> <p>Statement introduced in Junos OS Release 14.2 for MX series Routers with MPC.</p>
Description	Configure the interval for host-query message timeouts.
Options	<p><i>seconds</i>—Time interval. This value must be greater than the interval set for <i>query-response-interval</i>.</p> <p>Range: 1 through 1024</p> <p>Default: 125 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>Example: Configuring IGMP Snooping</i> • query-last-member-interval (Bridge Domains) on page 212 • query-response-interval (Bridge Domains) on page 213 • <i>mld-snooping</i> • <i>igmp-snooping</i>

query-last-member-interval (Bridge Domains)

Syntax	<code>query-last-member-interval seconds;</code>
Hierarchy Level	<pre>[edit bridge-domains <i>bridge-domain-name</i> protocols mld-snooping] , [edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface <i>interface-name</i>], [edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping vlan <i>vlan-id</i> interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols mld-snooping] [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping vlan <i>vlan-id</i> [edit routing-instances <i>routing-instance-name</i> protocols mld-snooping]interface <i>interface-name</i>] [edit protocols igmp-snooping vlan],</pre>
Release Information	<p>Statement introduced in Junos OS Release 8.5.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX series.</p> <p>Statement introduced in Junos OS Release 14.2 for MX series Routers with MPC.</p>
Description	Configure the interval for group-specific query timeouts.
Options	<p>seconds—Time interval, in fractions of a second or seconds.</p> <p>Range: 0.1 through 0.9, then in 1-second intervals 1 through 1024</p> <p>Default: 1 second</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</i> • query-interval on page 211 • query-response-interval on page 213 • <i>mld-snooping</i> • <i>igmp-snooping</i>

query-response-interval (Bridge Domains)

Syntax	<code>query-response-interval seconds;</code>
Hierarchy Level	<p>[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface interface-name],</p> <p>[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping vlan vlan-id interface interface-name],</p> <p>[edit bridge-domains <i>bridge-domain-name</i> protocols mld-snooping] ,</p> <p>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface interface-name],</p> <p>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping vlan vlan-id</p> <p>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols mld-snooping]interface interface-name]</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols mld-snooping]</p> <p>[edit protocols igmp-snooping vlan],</p>
Release Information	<p>Statement introduced in Junos OS Release 8.5.</p> <p>Statement introduced in Junos OS Release 13.2 for the QFX series.</p> <p>Statement introduced in Junos OS Release 14.2 for MX series Routers with MPC.</p>
Description	Specify how long to wait to receive a response to a specific query message from a host.
Options	<p><i>seconds</i>—Time interval. This interval should be less than the host-query interval.</p> <p>Range: 1 through 1024</p> <p>Default: 10 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>Example: Configuring IGMP Snooping</i> • query-interval (Bridge Domains) on page 211 • query-last-member-interval (Bridge Domains) on page 212 • <i>mld-snooping</i> • <i>igmp-snooping</i>

robust-count (Bridge Domains)

Syntax	<code>robust-count <i>number</i>;</code>
Hierarchy Level	<code>[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface <i>interface-name</i>],</code> <code>[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping vlan <i>vlan-id</i> interface <i>interface-name</i>],</code> <code>[edit bridge-domains <i>bridge-domain-name</i> protocols mld-snooping] ,</code> <code>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface <i>interface-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping vlan <i>vlan-id</i> interface <i>interface-name</i>]</code> <code>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols mld-snooping]</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols mld-snooping]</code>
Release Information	Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 14.2 for MX series Routers with MPC.
Description	Provide fine-tuning to allow for expected packet loss on a subnet. You can wait more intervals if subnet packet loss is high and IGMP or MLD report messages might be lost.
Options	<i>number</i> —Robust interval. 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>Example: Configuring IGMP Snooping</i>• <i>mld-snooping</i>• <i>igmp-snooping</i>

source (Bridge Domains)

Syntax	<code>source ip-address;</code>
Hierarchy Level	[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface interface-name static group], [edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface interface-name static group], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface interface-name static group], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols vlan vlan-id igmp-snooping interface interface-name static group]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Statically define multicast group source addresses on an interface.
Options	<i>ip-address</i> —IP address to use as the source for the 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"> <i>Example: Configuring IGMP Snooping</i>

source-address

Syntax	<code>source-address ip-address;</code>
Hierarchy Level	[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping proxy], [edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping vlan vlan-id proxy], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping proxy], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping vlan vlan-id proxy]
Release Information	Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 13.2 for the QFX series.
Description	Specify the IP address to use as the source for IGMP snooping reports in proxy mode. Reports are sent with address 0.0.0.0 as the source address unless there is a source address configured. You can also use this statement to configure the source address to use for IGMP snooping queries.
Options	<i>ip-address</i> —IP address to use as the source for proxy-mode IGMP snooping reports.
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</i>

static (Bridge Domains)

Syntax	<pre>static { group multicast-group-address { source ip-address; } }</pre>
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 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 igmp-snooping vlan <i>vlan-id</i> interface <i>interface-name</i>]</p>
Release Information	Statement introduced in Junos OS Release 8.5.
Description	<p>Define static multicast groups on an 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</i>

traceoptions (Protocols IGMP Snooping)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable> ; flag <i>flag</i> (detail disable receive send); } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> bridge-domains <i>domain-name</i> protocols igmp-snooping],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> bridge-domains <i>domain-name</i> protocols igmp-snooping],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols igmp-snooping],</p> <p>[edit bridge-domains <i>domain-name</i> protocols igmp-snooping],</p> <p>[edit routing-instances <i>instance-name</i> bridge-domains <i>domain-name</i> protocols igmp-snooping],</p> <p>[edit routing-instances <i>instance-name</i> protocols igmp-snooping]</p>
Release Information	Statement introduced in Junos OS Release 8.5.
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. All files are placed in the directory /var/log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached (xk to specify KB, xm to specify MB, or xg to specify gigabytes), at which point the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i> —Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> • all—All tracing operations. • client-notification—Trace notifications. • general—Trace general IGMP snooping protocol events. • group—Trace group operations. • host-notification—Trace host notifications. • leave—Trace leave group messages (IGMPv2 only). • normal—Trace normal IGMP snooping protocol events. • packets—Trace all IGMP packets.

- **policy**—Trace policy processing.
- **query**—Trace IGMP membership query messages.
- **report**—Trace membership report messages.
- **route**—Trace routing information.
- **state**—Trace IGMP state transitions.
- **task**—Trace routing protocol task processing.
- **timer**—Trace routing protocol timer processing.

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

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

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

Range: 10 KB through 1 gigabytes

Default: 128 KB

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

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

Related Documentation	<ul style="list-style-type: none">• <i>Configuring IGMP Snooping Trace Operations</i>• <i>Configuring IGMP Snooping</i>
------------------------------	--

vlan (Bridge Domains)

Syntax	<pre> vlan <i>vlan-id</i> { all immediate-leave; interface <i>interface-name</i> { group-limit <i>limit</i>; host-only-interface; multicast-router-interface; static { group <i>mcast-group-address</i> { source <i>ip-address</i>; } } } proxy { source-address <i>ip-address</i>; } query-interval <i>seconds</i>; query-last-member-interval <i>seconds</i>; query-response-interval <i>seconds</i>; robust-count <i>number</i>; } </pre>
Hierarchy Level	[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping], [edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping]
Release Information	Statement introduced in Junos OS Release 8.5. Statement introduced in Junos OS Release 13.2 for the QFX series.
Description	Configure IGMP snooping parameters for a particular VLAN.
Default	By default, IGMP snooping options apply to all VLANs.
Options	<i>vlan-id</i> —Apply the parameters to this VLAN. 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 VLAN-Specific IGMP Snooping Parameters igmp-snooping

Configuration Statements: MLD

- [mld](#) on page 222
- [accounting \(Protocols MLD Interface\)](#) on page 223
- [accounting \(Protocols MLD\)](#) on page 223
- [disable \(Protocols MLD\)](#) on page 224
- [exclude \(Protocols MLD\)](#) on page 224
- [group \(Protocols MLD\)](#) on page 225
- [group-count \(Protocols MLD\)](#) on page 226
- [group-increment \(Protocols MLD\)](#) on page 226
- [group-limit \(MLD\)](#) on page 227
- [group-policy \(Protocols MLD\)](#) on page 228
- [group-threshold \(Protocols MLD Interface\)](#) on page 229
- [immediate-leave \(Protocols MLD\)](#) on page 230
- [interface \(Protocols MLD\)](#) on page 231
- [log-interval \(Protocols MLD Interface\)](#) on page 232
- [maximum-transmit-rate \(Protocols MLD\)](#) on page 233
- [oif-map \(MLD Interface\)](#) on page 233
- [passive \(MLD\)](#) on page 234
- [query-interval \(Protocols MLD\)](#) on page 235
- [query-last-member-interval \(Protocols MLD\)](#) on page 236
- [query-response-interval \(Protocols MLD\)](#) on page 237
- [robust-count \(Protocols MLD\)](#) on page 238
- [source \(Protocols MLD\)](#) on page 238
- [source-count \(Protocols MLD\)](#) on page 239
- [source-increment \(Protocols MLD\)](#) on page 239
- [ssm-map \(Protocols MLD\)](#) on page 240
- [ssm-map-policy \(MLD\)](#) on page 240
- [static \(Protocols MLD\)](#) on page 241
- [version \(Protocols MLD\)](#) on page 242

mld

Syntax	<pre> mld { accounting; interface <i>interface-name</i> { (accounting no-accounting); disable; group-limit <i>limit</i>; group-policy [<i>policy-names</i>]; immediate-leave; oif-map [<i>map-names</i>]; passive; ssm-map <i>ssm-map-name</i>; ssm-map-policy <i>ssm-map-policy-name</i>; static (Protocols MLD) { 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>; } maximum-transmit-rate <i>packets-per-second</i>; query-interval <i>seconds</i>; query-last-member-interval <i>seconds</i>; query-response-interval <i>seconds</i>; robust-count <i>number</i>; } </pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols], [edit protocols]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Enable MLD on the routing device. MLD must be enabled for the routing device to receive multicast packets.
Default	MLD is disabled on the routing device. MLD is automatically enabled on all broadcast interfaces when you configure Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP).
Options	The statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

Related Documentation • *Enabling MLD*

accounting (Protocols MLD Interface)

Syntax	(accounting no-accounting);
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld interface interface-name], [edit protocols mld interface interface-name]
Release Information	Statement introduced in Junos OS Release 9.1.
Description	Enable or disable the collection of MLD 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	• <i>Example: Recording MLD Join and Leave Events</i>

accounting (Protocols MLD)

Syntax	accounting;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld], [edit protocols mld]
Release Information	Statement introduced in Junos OS Release 9.1.
Description	Enable the collection of MLD 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	• <i>Example: Recording MLD Join and Leave Events</i>


disable (Protocols MLD)

Syntax	disable;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld interface <i>interface-name</i>], [edit protocols mld interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Disable MLD 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 MLD</i>

exclude (Protocols MLD)

Syntax	exclude;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld interface <i>interface-name</i> static (Protocols MLD) group <i>multicast-group-address</i>], [edit protocols mld interface <i>interface-name</i> static (Protocols MLD) group <i>multicast-group-address</i>]
Release Information	Statement introduced in Junos OS Release 9.3.
Description	Configure the static group to operate in exclude mode. In exclude mode all sources except the address configured are accepted for the group. By default, the group operates in include mode.
Required Privilege Level	view-level—To view this statement in the configuration. control-level—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Enabling MLD Static Group Membership</i>

group (Protocols MLD)

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 mld interface <i>interface-name</i> static (Protocols MLD)], [edit protocols mld interface <i>interface-name</i> static (Protocols MLD)]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	The MLD multicast group address and (optionally) the source address for the multicast group being statically configured on an interface.
Options	<i>multicast-group-address</i> —Address of the group.
<div>  NOTE: You must specify a unique address for each group. </div>	
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 MLD Static Group Membership</i>

group-count (Protocols MLD)

Syntax	<code>group-count <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols <code>mld interface <i>interface-name</i> static (Protocols MLD) group <i>mcast-group-address</i></code>], [edit protocols <code>mld interface <i>interface-name</i> static (Protocols MLD) group <i>mcast-group-address</i></code>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Configure the number of static groups to be created.
Options	<i>number</i> —Number of static groups. Default: 1 Range: 1 through 512
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 MLD Static Group Membership</i>

group-increment (Protocols MLD)

Syntax	<code>group-increment <i>increment</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols <code>mld interface <i>interface-name</i> static (Protocols MLD) group <i>mcast-group-address</i></code>], [edit protocols <code>mld interface <i>interface-name</i> static (Protocols MLD) group <i>mcast-group-address</i></code>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Configure the number of times the address should be incremented for each static group created. The increment is specified in a format similar to an IPv6 address.
Options	<i>increment</i> —Number of times the address should be incremented. Default: ::1 Range: ::1 through ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:
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 MLD Static Group Membership</i>

group-limit (MLD)

Syntax	<code>group-limit <i>limit</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols mld interface <i>interface-name</i>]</p> <p>[edit protocols mld interface <i>interface-name</i>]</p> <p>[edit protocols mld-snooping vlan <i>vlan-name</i> interface <i>interface-name</i>]</p> <p>[edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-name</i> interface <i>interface-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.4.</p> <p>Support at the [edit protocols mld-snooping vlan <i>vlan-name</i> interface <i>interface-name</i>] and the [edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-name</i> interface <i>interface-name</i>] hierarchy levels introduced in Junos OS Release 13.3 for EX Series switches.</p> <p>Support at the [edit bridge-domains] hierarchy level introduced in Junos OS Release 14.2.</p>
Description	<p>Configure a limit for the number of multicast groups (or [S,G] channels in MLDv2) allowed on a logical interface. After this limit is reached, new reports are ignored and all related flows are not flooded on the interface.</p> <p>To confirm the configured group limit on the interface, use the show mld interface command.</p>
Default	By default, there is no limit to the number of multicast groups that can join the interface.
Options	<p><i>limit</i>—a 32-bit number for the limit on the interface.</p> <p>Range: 1 through 32,767.</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 the Number of MLD Multicast Group Joins on Logical Interfaces</i>


group-policy (Protocols MLD)

Syntax	<code>group-policy [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld interface <i>interface-name</i>], [edit protocols mld interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.1.
Description	When a routing device running MLD version 1 or version 2 (MLDv1 or MLDv2), receives an MLD report, the routing device compares the group against the specified group policy and performs the action configured in that policy (for example, rejects the report).
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 Unwanted MLD Reports at the MLD Interface Level</i>

group-threshold (Protocols MLD Interface)

Syntax	<code>group-threshold value;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld interface interface-name], [edit protocols mld interface interface-name]
Release Information	Statement introduced in Junos OS Release 12.2.
Description	<p>Specify the threshold at which a warning message is logged for the multicast groups received on a logical interface. The threshold is a percentage of the maximum number of multicast groups allowed on a logical interface.</p> <p>For example, if you configure a maximum number of 1,000 incoming multicast groups, and you configure a threshold value of 90 percent, warning messages are logged in the system log when the interface receives 900 groups.</p> <p>To confirm the configured group threshold on the interface, use the show mld interface command.</p>
Default	By default, there is no configured threshold value.
Options	<p>value—Percentage of the maximum number of multicast groups allowed on the interface that starts triggering the warning. You configure a percentage of the group-limit value that starts triggering the warnings. You must explicitly configure the group-limit to configure a threshold value.</p> <p>Range: 1 through 100</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 the Number of MLD Multicast Group Joins on Logical Interfaces</i> • group-limit on page 227 • log-interval on page 232

immediate-leave (Protocols MLD)

Syntax	immediate-leave;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld interface <i>interface-name</i>], [edit protocols mld interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 8.3.
Description	<p>The immediate leave setting is useful for minimizing the leave latency of MLD 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 MLD 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 MLD group-specific queries to the interface. The interface is pruned from the multicast tree for the multicast group specified in the MLD 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 MLD version 1 and MLD version 2.</p>
	<div>  <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 routing device only knows about the one interested host and does not know about the others.</p> </div>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> <i>Specifying Immediate-Leave Host Removal for MLD</i>

interface (Protocols MLD)

Syntax	<pre> interface <i>interface-name</i> { disable; (accounting no-accounting); group-limit <i>limit</i>; group-policy [<i>policy-names</i>]; group-threshold <i>value</i>; immediate-leave; log-interval <i>seconds</i>; oif-map [<i>map-names</i>]; passive; ssm-map <i>ssm-map-name</i>; ssm-map-policy <i>ssm-map-policy-name</i>; static (Protocols MLD) { 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 mld], [edit protocols mld]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Enable MLD on an interface and configure interface-specific properties.
Options	<p><i>interface-name</i>—Name of the interface. Specify the full interface name, including the physical and logical address components. To configure all interfaces, you can specify all.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Enabling MLD

log-interval (Protocols MLD Interface)

Syntax	log-interval <i>seconds</i> ;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld interface <i>interface-name</i>], [edit protocols mld interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 12.2.
Description	<p>Specify the minimum time interval (in seconds) between sending consecutive log messages to the system log for multicast groups. To configure the time interval, you must specify the maximum number of multicast groups allowed on the interface.</p> <p>To confirm the configured log interval on the interface, use the show mld interface command.</p>
Default	By default, there is no configured time interval.
Options	<p>seconds—Minimum time interval (in seconds) between log messages. You must explicitly configure the group-limit to configure a time interval to send log messages.</p> <p>Range: 6 through 32,767 seconds</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 the Number of MLD Multicast Group Joins on Logical Interfaces</i>• group-limit on page 227• group-threshold on page 229

maximum-transmit-rate (Protocols MLD)

Syntax	<code>maximum-transmit-rate <i>packets-per-second</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld], [edit protocols mld]
Release Information	Statement introduced in Junos OS Release 9.3.
Description	Limit the transmission rate of MLD packets.
Options	<p>packets-per-second—Maximum number of MLD packets transmitted in one second by the routing device.</p> <p>Range: 1 through 10000</p> <p>Default: 500 packets</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>Limiting the Maximum MLD Message Rate</i>

oif-map (MLD Interface)

Syntax	<code>oif-map <i>map-name</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld interface <i>interface-name</i>], [edit protocols mld interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Associate an outgoing interface (OIF) map to an MLD logical interface. The OIF map is a routing policy statement that can contain multiple terms.
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 Multicast with Subscriber VLANs</i>

passive (MLD)

Syntax	<code>passive <allow-receive> <send-general-query> <send-group-query>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld interface <i>interface-name</i>], [edit protocols mld interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6. allow-receive , send-general-query , and send-group-query options added in Junos OS Release 10.0.
Description	Specify that MLD run on the interface and either not send and receive control traffic or selectively send and receive control traffic such as MLD reports, queries, and leaves.



NOTE: You can selectively activate up to two out of the three available options for the **passive** statement while keeping the other functions **passive** (inactive). Activating all three options is equivalent to not using the **passive** statement.

Options	allow-receive —Enables MLD to receive control traffic on the interface. send-general-query —Enables MLD to send general queries on the interface. send-group-query —Enables MLD to send group-specific and group-source-specific queries on the interface.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><i>Example: Configuring Multicast with Subscriber VLANs</i>

query-interval (Protocols MLD)

Syntax	query-interval <i>seconds</i> ;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld], [edit protocols mld] [edit protocols mld-snooping vlan <i>vlan-id</i>] [edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-id</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Support at the [edit protocols mld-snooping vlan <i>vlan-id</i>] and the [edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-id</i>] hierarchy levels introduced in Junos OS Release 13.3 for EX Series switches.
Description	Specify how often the querier routing device sends general host-query messages.
Options	<i>seconds</i> —Time interval. This value must be greater than the interval set for query-response-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 MLD Host-Query Message Interval</i> • query-last-member-interval (Protocols MLD) on page 236 • query-response-interval (Protocols MLD) on page 237

query-last-member-interval (Protocols MLD)

Syntax	query-last-member-interval <i>seconds</i> ;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld], [edit protocols mld] [edit protocols mld-snooping <i>vlan</i> <i>vlan-id</i>] [edit routing-instances <i>instance-name</i> protocols mld-snooping <i>vlan</i> <i>vlan-id</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Support at the [edit protocols mld-snooping <i>vlan</i> <i>vlan-id</i>] and the [edit routing-instances <i>instance-name</i> protocols mld-snooping <i>vlan</i> <i>vlan-id</i>] hierarchy levels introduced in Junos OS Release 13.3 for EX Series switches.
Description	Specify how often the querier routing device sends group-specific query messages.
Options	<i>seconds</i> —Time interval, in fractions of a second or seconds. Range: 0.1 through 0.9, then in 1-second intervals from 1 through 1024 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 MLD Last-Member Query Interval</i>• query-interval (Protocols MLD) on page 235• query-response-interval (Protocols MLD) on page 237

query-response-interval (Protocols MLD)

Syntax	<code>query-response-interval seconds;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols mld],</p> <p>[edit protocols mld]</p> <p>[edit protocols mld-snooping vlan <i>vlan-id</i>]</p> <p>[edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-id</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>Support at the [edit protocols mld-snooping vlan <i>vlan-id</i>] and the [edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-id</i>] hierarchy levels introduced in Junos OS Release 13.3 for EX Series switches.</p>
Description	Specify how long the querier routing device waits to receive a response to a host-query message from a host.
Options	<p><i>seconds</i>—Time interval.</p> <p>Range: 1 through 1024</p> <p>Default: 10 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>Modifying the MLD Query Response Interval</i> • query-interval (Protocols MLD) on page 235 • query-last-member-interval (Protocols MLD) on page 236

robust-count (Protocols MLD)

Syntax	<code>robust-count <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld], [edit protocols mld]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Tune for the expected packet loss on a subnet.
Options	<i>number</i> —Time interval. This interval must be less than the interval between general host-query messages. Range: 2 through 10 Default: 2 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: Modifying the MLD Robustness Variable</i>

source (Protocols MLD)

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 mld interface <i>interface-name</i> static (Protocols MLD) group <i>mcast-group-address</i>], [edit protocols mld interface <i>interface-name</i> static (Protocols MLD) group <i>mcast-group-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	IP version 6 (IPv6) unicast source address for the multicast group being statically configured on an interface.
Options	<i>ip-address</i> —One or more IPv6 unicast 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>Enabling MLD Static Group Membership</i>

source-count (Protocols MLD)

Syntax	<code>source-count <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld interface interface-name static (Protocols MLD) group multicast-group-address source], [edit protocols mld interface interface-name static (Protocols MLD) group multicast-group-address source]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Configure the number of multicast source addresses that should be accepted for each static group created.
Options	<i>number</i> —Number of source addresses. Default: 1 Range: 1 through 1024
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Enabling MLD Static Group Membership

source-increment (Protocols MLD)

Syntax	<code>source-increment <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld interface interface-name static (Protocols MLD) group multicast-group-address source], [edit protocols mld interface interface-name static (Protocols MLD) group multicast-group-address source]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Configure the number of times the address should be incremented for each static group created. The increment is specified in a format similar to an IPv6 address.
Options	<i>increment</i> —Number of times the source address should be incremented. Default: ::1 Range: ::1 through ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Enabling MLD Static Group Membership

ssm-map (Protocols MLD)

Syntax	<code>ssm-map <i>ssm-map-name</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld interface interface-name], [edit protocols mld interface interface-name]
Release Information	Statement introduced in Junos OS Release 7.4.
Description	Apply an SSM map to an MLD 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>

ssm-map-policy (MLD)

Syntax	<code>ssm-map-policy <i>ssm-map-policy-name</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld interface interface-name], [edit protocols mld interface interface-name]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Apply an SSM map policy to an MLD interface.
Options	<i>ssm-map-policy-name</i> —Name of SSM map policy.
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 Maps for Different Groups to Different Sources</i>

static (Protocols MLD)

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 **mld interface** *interface-name*],
[edit protocols **mld interface** *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Test multicast forwarding on an interface.

The **static** statement simulates MLD joins on a routing device statically on an interface without any MLD hosts. It is supported for both MLDv1 and MLDv2 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 MLD Static Group Membership*

version (Protocols MLD)

Syntax	<code>version version;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols <code>mld interface interface-name</code>], [edit protocols <code>mld interface interface-name</code>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the MLD version explicitly. MLD version 2 (MLDv2) is used only to support source-specific multicast (SSM).
Options	version —MLD version to run on the interface. Range: 1 or 2 Default: 1 (MLDv1)
Required Privilege Level	routing and trace—To view this statement in the configuration. routing-control and trace-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Modifying the MLD Version</i>

CHAPTER 15

Configuration Statements: MLD Snooping

- [mld-snooping](#) on page 244
- [group \(MLD Snooping\)](#) on page 245
- [group-limit \(MLD\)](#) on page 246
- [host-only-interface](#) on page 247
- [immediate-leave \(MLD Snooping\)](#) on page 248
- [interface \(MLD Snooping\)](#) on page 249
- [multicast-router-interface \(MLD Snooping\)](#) on page 250
- [qualified-vlan \(MLD Snooping\)](#) on page 250
- [query-interval \(Protocols MLD\)](#) on page 251
- [query-last-member-interval \(Protocols MLD\)](#) on page 252
- [query-response-interval \(Protocols MLD\)](#) on page 253
- [robust-count \(MLD Snooping\)](#) on page 254
- [static \(MLD Snooping\)](#) on page 255
- [traceoptions \(MLD Snooping\)](#) on page 256
- [vlan \(MLD Snooping\)](#) on page 259

mld-snooping

Syntax	<pre> mld-snooping { vlan (vlan-name) { immediate-leave; interface (all interface-name) { group-limit limit; host-only-interface; immediate-leave; multicast-router-interface; static { group ip-address { source ip-address; } } } } qualified-vlan vlan-id; query-interval seconds; query-last-member-interval seconds; query-response-interval seconds; robust-count number; traceoptions { file filename <files number> <size size> <world-readable no-world-readable>; flag flag <flag-modifier>; } } </pre>
Hierarchy Level	[edit protocols] [edit routing-instances <i>instance-name</i> protocols]
Release Information	Statement introduced in Junos OS Release 13.3 for EX Series switches.
Description	<p>Enable and configure MLD snooping.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring MLD Snooping on EX Series Switches on page 60 • Configuring MLD Snooping on a VLAN (CLI Procedure) on page 54

group (MLD Snooping)

Syntax	<code>group <i>multicast-group-address</i> { source <i>ip-address</i>; }</code>
Hierarchy Level	[edit protocols mld-snooping <i>vlan</i> (all <i>vlan-name</i>) <i>interface</i> (all <i>interface-name</i>) <i>static</i>] [edit routing-instances <i>instance-name</i> protocols <i>mld-snooping vlan vlan-name interface interface-name static</i>]
Release Information	Statement introduced in Junos OS Release 12.1 for EX Series switches. Support at the [edit routing-instances <i>instance-name</i> protocols <i>mld-snooping vlan vlan-name interface interface-name static</i>] hierarchy level introduced in Junos OS Release 13.3 for EX Series switches. Support for the source statement introduced in Junos OS Release 13.3 for EX Series switches.
Description	Configure a static multicast group on an interface and (optionally) the source address for the multicast group.
Options	<i>multicast-group-address</i> —Valid IP multicast address for the multicast group. <i>source ip-address</i> —Valid IP multicast address for the source of 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"> • <i>Configuring MLD Snooping on a VLAN (CLI Procedure)</i>


group-limit (MLD)

Syntax	<code>group-limit limit;</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> protocols mld interface <i>interface-name</i>]</code> <code>[edit protocols mld interface <i>interface-name</i>]</code> <code>[edit protocols mld-snooping vlan <i>vlan-name</i> interface <i>interface-name</i>]</code> <code>[edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-name</i> interface <i>interface-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 10.4. Support at the <code>[edit protocols mld-snooping vlan <i>vlan-name</i> interface <i>interface-name</i>]</code> and the <code>[edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-name</i> interface <i>interface-name</i>]</code> hierarchy levels introduced in Junos OS Release 13.3 for EX Series switches. Support at the <code>[edit bridge-domains]</code> hierarchy level introduced in Junos OS Release 14.2.
Description	Configure a limit for the number of multicast groups (or [S,G] channels in MLDv2) allowed on a logical interface. After this limit is reached, new reports are ignored and all related flows are not flooded on the interface. To confirm the configured group limit on the interface, use the <code>show mld interface</code> command.
Default	By default, there is no limit to the number of multicast groups that can join the interface.
Options	<i>limit</i> —a 32-bit number for the limit on the interface. Range: 1 through 32,767.
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 the Number of MLD Multicast Group Joins on Logical Interfaces</i>

host-only-interface

Syntax	host-only-interface;
Hierarchy Level	<p>[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface interface-name],</p> <p>[edit bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping vlan vlan-id interface interface-name],</p> <p>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols igmp-snooping interface interface-name],</p> <p>[edit routing-instances <i>routing-instance-name</i> bridge-domains <i>bridge-domain-name</i> protocols vlan vlan-id igmp-snooping interface interface-name]</p> <p>[edit protocols igmp-snooping vlan interface]</p> <p>[edit protocols mld-snooping vlan vlan-id interface <i>interface-name</i>]</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols mld-snooping vlan vlan-id 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 13.2 for the QFX series.</p> <p>Support at the [edit protocols mld-snooping vlan vlan-id interface interface-name] and the [edit routing-instances <i>routing-instance-name</i> protocols mld-snooping vlan vlan-id interface interface-name] hierarchy levels introduced in Junos OS Release 13.3 for EX Series switches.</p>
Description	Configure an interface as a host-facing interface. IGMP and MLD queries received on these interfaces are dropped.
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"> • Example: Configuring IGMP Snooping • multicast-router-interface on page 209

immediate-leave (MLD Snooping)

Syntax	<code>immediate-leave;</code>
Hierarchy Level	<code>[edit protocols mld-snooping vlan (all vlan-name)]</code> <code>[edit protocols mld-snooping vlan vlan-name interface interface-name]</code> <code>[edit routing-instances instance-name protocols mld-snooping vlan vlan-name interface interface-name]</code>
Release Information	<p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p> <p>Support at the <code>[edit protocols mld-snooping vlan vlan-name interface interface-name]</code> and the <code>[edit routing-instances instance-name protocols mld-snooping vlan vlan-name interface interface-name]</code> hierarchy levels introduced in Junos OS Release 13.3 for EX Series switches.</p> <p>Support at</p>
Description	<p>Configure MLD snooping immediate leave for the specified VLAN or interface. When you configure immediate leave, host tracking is enabled, which allows the switch to track the hosts that send join messages. 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 message from a host, it sends out a group membership query to all hosts. If it does not receive any join group reports on the interface in response to the group membership query within a set interval, it then stops forwarding multicast traffic to the interface.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;"> <p> NOTE: Immediate leave is supported for both MLD version 1 (MLDv1) and MLDv2. However, with MLDv1, we recommend that you configure immediate leave only when there is only one MLD host on an interface. In MLDv1, only one host on a interface sends a join report in response to a group membership query—any other interested hosts suppress their reports. This report-suppression feature means that the switch only knows about one interested host on the interface at any given time.</p> </div>
Default	The immediate-leave feature is disabled.
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 MLD Snooping on a VLAN (CLI Procedure)</i>

interface (MLD Snooping)

Syntax	<pre> interface (all <i>interface-name</i>) { group-limit <i>limit</i>; host-only-interface; immediate-leave; multicast-router-interface; static { group <i>ip-address</i> { source <i>ip-address</i>; } } } </pre>
Hierarchy Level	[edit protocols mld-snooping vlan (all <i>vlan-name</i>)] [edit routing-instances <i>instance-name</i> protocols mld-snooping vlan (<i>vlan-name</i>)]
Release Information	<p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p> <p>Support at the [edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-name</i>] hierarchy introduced in Junos OS Release 13.3 for EX Series switches.</p> <p>Support for the group-limit, host-only-interface, and the immediate-leave statements introduced in Junos OS Release 13.3 for EX Series switches.</p>
Description	For MLD snooping, configure an interface as a static multicast-router interface, a host-side interface, or a static member of a multicast group.
Options	<p>all—(All EX Series switches except EX9200) 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"> Configuring MLD Snooping on a VLAN (CLI Procedure)

multicast-router-interface (MLD Snooping)

Syntax	<code>multicast-router-interface;</code>
Hierarchy Level	<code>[edit protocols mld-snooping vlan (all <i>vlan-name</i>) interface (all <i>interface-name</i>)]</code> <code>[edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-name</i> interface <i>interface-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 12.1 for EX Series switches. Support at the <code>[edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-name</i> interface <i>interface-name</i>]</code> hierarchy level introduced in Junos OS Release 13.3 for EX Series switches.
Description	Statically configure the interface as a multicast-router interface—that is, an interface that faces towards a multicast router or other MLD querier.



NOTE: If the specified interface is a trunk port, the interface becomes a multicast-router 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 router interface, even if the interface is configured as a multicast-router interface only for MLD snooping.

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 MLD Snooping on a VLAN (CLI Procedure)

qualified-vlan (MLD Snooping)

Syntax	<code>qualified-vlan <i>vlan-id</i>;</code>
Hierarchy Level	<code>[edit protocols mld-snooping vlan <i>vlan-name</i>]</code> <code>[edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 13.3 for EX Series switches.
Description	Configure VLAN options for qualified learning.
Options	<i>vlan-id</i> —VLAN ID of the learning domain. Range: 0 through 1023
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 MLD Snooping on a VLAN (CLI Procedure) on page 54 • show mld snooping membership on page 453

query-interval (Protocols MLD)

Syntax	query-interval <i>seconds</i> ;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld], [edit protocols mld] [edit protocols mld-snooping vlan <i>vlan-id</i>] [edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-id</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Support at the [edit protocols mld-snooping vlan <i>vlan-id</i>] and the [edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-id</i>] hierarchy levels introduced in Junos OS Release 13.3 for EX Series switches.
Description	Specify how often the querier routing device sends general host-query messages.
Options	<i>seconds</i> —Time interval. This value must be greater than the interval set for query-response-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 MLD Host-Query Message Interval</i> • query-last-member-interval (Protocols MLD) on page 236 • query-response-interval (Protocols MLD) on page 237

query-last-member-interval (Protocols MLD)

Syntax	query-last-member-interval <i>seconds</i> ;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols mld], [edit protocols mld] [edit protocols mld-snooping vlan <i>vlan-id</i>] [edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-id</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Support at the [edit protocols mld-snooping vlan <i>vlan-id</i>] and the [edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-id</i>] hierarchy levels introduced in Junos OS Release 13.3 for EX Series switches.
Description	Specify how often the querier routing device sends group-specific query messages.
Options	<i>seconds</i> —Time interval, in fractions of a second or seconds. Range: 0.1 through 0.9, then in 1-second intervals from 1 through 1024 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 MLD Last-Member Query Interval</i>• query-interval (Protocols MLD) on page 235• query-response-interval (Protocols MLD) on page 237

query-response-interval (Protocols MLD)

Syntax	<code>query-response-interval seconds;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols mld],</p> <p>[edit protocols mld]</p> <p>[edit protocols mld-snooping vlan <i>vlan-id</i>]</p> <p>[edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-id</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>Support at the [edit protocols mld-snooping vlan <i>vlan-id</i>] and the [edit routing-instances <i>instance-name</i> protocols mld-snooping vlan <i>vlan-id</i>] hierarchy levels introduced in Junos OS Release 13.3 for EX Series switches.</p>
Description	Specify how long the querier routing device waits to receive a response to a host-query message from a host.
Options	<p><i>seconds</i>—Time interval.</p> <p>Range: 1 through 1024</p> <p>Default: 10 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>Modifying the MLD Query Response Interval</i> • query-interval (Protocols MLD) on page 235 • query-last-member-interval (Protocols MLD) on page 236

robust-count (MLD Snooping)

Syntax	<code>robust-count <i>number</i>;</code>
Hierarchy Level	<code>[edit protocols mld-snooping <i>vlan</i> (all <i>vlan-name</i>)]</code> <code>[edit routing-instances <i>instance-name</i> protocols mld-snooping <i>vlan</i> <i>vlan-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 12.1 for EX Series switches. Support at the <code>[edit routing-instances <i>instance-name</i> protocols mld-snooping <i>vlan</i> <i>vlan-name</i>]</code> hierarchy level introduced in Junos OS Release 13.3 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 MLD. The default for the MLD 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 MLD Snooping on a VLAN (CLI Procedure)</i>

static (MLD Snooping)

Syntax	static { group ip-address; }
Hierarchy Level	[edit protocols mld-snooping vlan (all vlan-name) interface (all interface-name)] [edit routing-instances instance-name protocols mld-snooping vlan vlan-name interface interface-name]
Release Information	Statement introduced in Junos OS Release 12.1 for EX Series switches. Support at the [edit routing-instances instance-name protocols mld-snooping vlan vlan-name interface interface-name] hierarchy level introduced in Junos OS Release 13.3 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"> Configuring MLD Snooping on a VLAN (CLI Procedure)

traceoptions (MLD 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> <<i>flag-modifier</i>>; } </pre>
Hierarchy Level	<p>[edit protocols mld-snooping]</p> <p>[edit protocols mld-snooping <i>vlan</i> <i>vlan-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p> <p>Support at the [edit protocols mld-snooping <i>vlan</i> <i>vlan-name</i>] hierarchy level introduced in Junos OS Release 13.3 for EX Series switches.</p>
Description	Define tracing operations for MLD 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 <i>/var/log</i>.</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. • client-notification—(EX9200 switches only) Trace client notifications. • general—Trace general MLD snooping protocol events. • group—(EX9200 switches only) Trace group operations. • host-notification—(EX9200 switches only) Trace host notifications. • krt—(All EX Series switches except EX9200) Trace communication over routing socket. • leave—Trace leave group messages. • nexthop—(All EX Series switches except EX9200) Trace events related to next-hops.

- **normal**—Trace normal MLD snooping protocol events. If you do not specify this flag, only unusual or abnormal operations are traced.
- **packets**—Trace all MLD packets.
- **policy**—Trace policy processing.
- **query**—Trace MLD membership query messages.
- **report**—Trace membership report messages.
- **route**—Trace routing information.
- **state**—Trace MLD state transitions.
- **task**—Trace routing protocol task processing.
- **timer**—Trace routing protocol timer processing.
- **vlan**—(All EX Series switches except EX9200) 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—(All EX Series switches except EX9200) (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—(All EX Series switches except EX9200) (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**

vlan (MLD Snooping)

Syntax	<pre> vlan (all <i>vlan-name</i>) { disable; immediate-leave; interface (all <i>interface-name</i>) { group-limit <i>limit</i>; host-only-interface; immediate-leave; multicast-router-interface; static { group <i>ip-address</i> { source <i>ip-address</i>; } } } qualified-vlan; query-interval <i>seconds</i>; query-last-member-interval <i>seconds</i>; query-response-interval <i>seconds</i>; robust-count <i>number</i>; traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i> <flag-modifier>; } version <i>version</i>; } </pre>
Hierarchy Level	<p>[edit protocols mld-snooping]</p> <p>[edit routing-instances <i>instance-name</i> protocols mld-snooping]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p> <p>Support at the [edit routing-instances <i>instance-name</i> protocols mld-snooping] hierarchy introduced in Junos OS Release 13.3 for EX Series switches.</p> <p>Support for the qualified-vlan, query-interval, query-last-member-interval, query-response-interval, and traceoptions statements introduced in Junos OS Release 13.3 for EX Series switches.</p>
Description	<p>Configure MLD snooping parameters for a VLAN.</p> <p>When the vlan configuration statement is used without the disable statement, MLD snooping is enabled on the specified VLAN or on all VLANs.</p>
Default	<p>If the vlan statement is not included in the configuration, MLD snooping is disabled.</p>
Options	<p>all—(All EX Series switches except EX9200) Configure MLD snooping parameters for all VLANs on the switch.</p> <p><i>vlan-name</i>—Configure MLD snooping parameters for the specified VLAN.</p>



TIP: When you configure MLD snooping parameters using the `vlan all` statement, any VLAN that is not individually configured for MLD snooping inherits the `vlan all` configuration. Any VLAN that is individually configured for MLD 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 {
  mld-snooping {
    vlan all {
      robust-count 8;
    }
    vlan employee {
      interface ge-0/0/8.0 {
        static {
          group ff1e::1;
        }
      }
    }
  }
}
```

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	routing—To view this statement in the configuration.
Level	routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring MLD Snooping on a VLAN (CLI Procedure)</i>

CHAPTER 16

Configuration Statements: MSDP

- [msdp](#) on page 262
- [active-source-limit](#) on page 264
- [authentication-key](#) on page 265
- [data-encapsulation](#) on page 266
- [default-peer](#) on page 267
- [disable](#) (Protocols MSDP) on page 268
- [export](#) (Protocols MSDP) on page 269
- [group](#) (Protocols MSDP) on page 270
- [hold-time](#) (Protocols MSDP) on page 271
- [import](#) (Protocols MSDP) on page 272
- [keep-alive](#) (Protocols MSDP) on page 273
- [local-address](#) (Protocols MSDP) on page 274
- [log-interval](#) (Protocols MSDP) on page 275
- [log-warning](#) (Protocols MSDP) on page 276
- [maximum](#) (MSDP Active Source Messages) on page 277
- [mode](#) (Protocols MSDP) on page 278
- [peer](#) (Protocols MSDP) on page 279
- [rib-group](#) (Protocols MSDP) on page 280
- [sa-hold-time](#) (Protocols MSDP) on page 281
- [source](#) (Protocols MSDP) on page 282
- [threshold](#) (MSDP Active Source Messages) on page 283
- [traceoptions](#) (Protocols MSDP) on page 284

msdp

```
Syntax  msdp {
        disable;
        active-source-limit {
            log-interval seconds;
            log-warning value;
            maximum number;
            threshold number;
        }
        data-encapsulation (disable | enable);
        export [ policy-names ];
        group group-name {
            ...group-configuration ...
        }
        hold-time seconds;
        import [ policy-names ];
        local-address address;
        keep-alive seconds;
        peer address {
            ...peer-configuration ...
        }
        rib-group group-name;
        source ip-prefix</prefix-length> {
            active-source-limit {
                maximum number;
                threshold number;
            }
        }
        sa-hold-time seconds;
        traceoptions {
            file filename <files number> <size size> <world-readable | no-world-readable>;
            flag flag <flag-modifier> <disable>;
        }
        group group-name {
            disable;
            export [ policy-names ];
            import [ policy-names ];
            local-address address;
            mode (mesh-group | standard);
            peer address {
                ... same statements as at the [edit protocols msdp peer address] hierarchy level shown
                just following ...
            }
            traceoptions {
                file filename <files number> <size size> <world-readable | no-world-readable>;
                flag flag <flag-modifier> <disable>;
            }
        }
        peer address {
            disable;
            active-source-limit {
                maximum number;
                threshold number;
            }
        }
    }
```



```

    }
    authentication-key peer-key;
    default-peer;
    export [ policy-names ];
    import [ policy-names ];
    local-address address;
    traceoptions {
        file filename <files number> <size size> <world-readable | no-world-readable>;
        flag flag <flag-modifier> <disable>;
    }
}
}

```

Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols], [edit protocols], [edit routing-instances <i>routing-instance-name</i> protocols]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.4 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	Enable MSDP on the router or switch. You must also configure at least one peer for MSDP to function.
Default	MSDP is disabled on the router or switch.
Options	The 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>Example: Configuring MSDP in a Routing Instance</i>

active-source-limit

Syntax	<pre>active-source-limit { log-interval seconds; log-warning value; maximum number; threshold number; }</pre>
Hierarchy Level	<pre>[edit logical-systems logical-system-name protocols msdp], [edit logical-systems logical-system-name protocols msdp group group-name peer address], [edit logical-systems logical-system-name protocols msdp peer address], [edit logical-systems logical-system-name protocols msdp source ip-address/prefix-length], [edit logical-systems logical-system-name routing-instances instance-name protocols msdp], [edit logical-systems logical-system-name routing-instances routing-instance-name protocols msdp group group-name peer address], [edit logical-systems logical-system-name routing-instances routing-instance-name protocols msdp peer address], [edit logical-systems logical-system-name routing-instances routing-instance-name protocols msdp source ip-address/prefix-length], [edit protocols msdp], [edit protocols msdp group group-name peer address], [edit protocols msdp peer address], [edit protocols msdp source ip-address/prefix-length], [edit routing-instances routing-instance-name protocols msdp], [edit routing-instances routing-instance-name protocols msdp group group-name peer address], [edit routing-instances routing-instance-name protocols msdp peer address], [edit routing-instances routing-instance-name protocols msdp source ip-address/prefix-length]</pre>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</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	Limit the number of active source messages the routing device accepts.
Default	If you do not include this statement, the router accepts any number of MSDP active source messages.
Options	The options are explained separately.
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 MSDP with Active Source Limits and Mesh Groups</i>

authentication-key

Syntax	<code>authentication-key peer-key;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols <code>msdp group group-name peer address</code>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols <code>msdp peer address</code>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols <code>msdp group group-name peer address</code>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols <code>msdp peer address</code>],</p> <p>[edit protocols <code>msdp group group-name peer address</code>],</p> <p>[edit protocols <code>msdp peer address</code>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols <code>msdp group group-name peer address</code>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols <code>msdp peer address</code>]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</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	Associate a Message Digest 5 (MD5) signature option authentication key with an MSDP peering session.
Default	If you do not include this statement, the routing device accepts any valid MSDP messages from the peer address.
Options	<p>peer-key—MD5 authentication key. The peer key can be a text string up to 16 letters and digits long. Strings can include any ASCII characters with the exception of (,), &, and [. If you include spaces in an MSDP authentication key, enclose all characters in quotation marks (" ").</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 MSDP in a Routing Instance</i>

data-encapsulation

Syntax	data-encapsulation (disable enable);
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols msdp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp], [edit protocols msdp], [edit routing-instances <i>routing-instance-name</i> protocols msdp]
Release Information	Statement introduced before Junos OS Release 7.4. 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	Configure a rendezvous point (RP) using MSDP to encapsulate multicast data received in MSDP register messages inside forwarded MSDP source-active messages.
Default	If you do not include this statement, the RP encapsulates multicast data.
Options	disable —(Optional) Do not use MSDP data encapsulation. enable —Use MSDP data encapsulation. Default: enable
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 MSDP with Active Source Limits and Mesh Groups</i>

default-peer

Syntax	default-peer;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp peer <i>address</i>],</p> <p>[edit protocols msdp],</p> <p>[edit protocols msdp group <i>group-name</i>],</p> <p>[edit protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit protocols msdp peer <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp peer <i>address</i>]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</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	Establish this peer as the default MSDP peer and accept source-active messages from the peer without the usual peer-reverse-path-forwarding (peer-RPF) check.
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 MSDP with Active Source Limits and Mesh Groups</i>

disable (Protocols MSDP)

Syntax	disable;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp peer <i>address</i>],</p> <p>[edit protocols msdp],</p> <p>[edit protocols msdp group <i>group-name</i>],</p> <p>[edit protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit protocols msdp peer <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp peer <i>address</i>]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</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	Explicitly disable MSDP.
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>Disabling MSDP</i>

export (Protocols MSDP)

Syntax	<code>export [<i>policy-names</i>];</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp peer <i>address</i>],</p> <p>[edit protocols msdp],</p> <p>[edit protocols msdp group <i>group-name</i>],</p> <p>[edit protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit protocols msdp peer <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp peer <i>address</i>]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</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	Apply one or more policies to routes being exported from the routing table into MSDP.
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 MSDP in a Routing Instance</i> • import on page 272

group (Protocols MSDP)

Syntax	<pre> group <i>group-name</i> { disable; export [<i>policy-names</i>]; import [<i>policy-names</i>]; local-address <i>address</i>; mode (mesh-group standard); traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i> <<i>flag-modifier</i>> <disable>; } peer <i>address</i>; { disable; active-source-limit { maximum <i>number</i>; threshold <i>number</i>; } authentication-key <i>peer-key</i>; default-peer; export [<i>policy-names</i>]; import [<i>policy-names</i>]; local-address <i>address</i>; traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i> <<i>flag-modifier</i>> <disable>; } } } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols msdp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp], [edit protocols msdp], [edit routing-instances <i>routing-instance-name</i> protocols msdp]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4. 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.</p>
Description	<p>Define an MSDP peer group. MSDP peers within groups share common tracing options, if present and not overridden for an individual peer with the peer statement. To configure multiple MSDP groups, include multiple group statements.</p> <p>By default, the group's options are identical to the global MSDP options. To override the global options, include group-specific options within the group statement.</p> <p>The group must contain at least one peer.</p>
Options	<p>group-name—Name of the MSDP group.</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

- *Example: Configuring MSDP in a Routing Instance*

hold-time (Protocols MSDP)

Syntax hold-time *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols msdp],
[edit logical-systems *logical-system-name* protocols msdp group *group-name* peer address],
[edit logical-systems *logical-system-name* protocols msdp peer address],
[edit logical-systems *logical-system-name* routing-instances *instance-name* protocols msdp],
[edit logical-systems *logical-system-name* routing-instances *instance-name* protocols msdp group *group-name* peer address],
[edit logical-systems *logical-system-name* routing-instances *instance-name* protocols msdp peer address],
[edit protocols msdp],
[edit protocols msdp group *group-name* peer address],
[edit protocols msdp peer address],
[edit routing-instances *instance-name* protocols msdp],
[edit routing-instances *instance-name* protocols msdp group *group-name* peer address]
[edit routing-instances *instance-name* protocols msdp peer address],

Release Information Statement introduced in Junos OS Release 12.3.

Description Specify the hold-time period to use when maintaining a connection with the MSDP peer. If a keepalive message is not received for the hold-time period, the MSDP peer connection is terminated. According to the RFC 3618, *Multicast Source Discovery Protocol (MSDP)*, the recommended value for the hold-time period is 75 seconds.

The hold-time period must be longer than the keepalive interval.

You might want to change the hold-time period and keepalive timer for consistency in a multi-vendor environment.

Default In Junos OS, the default hold-time period is 75 seconds, and the default keepalive interval is 60 seconds.

Options *seconds*—Hold time.
Range: 15 through 150 seconds
Default: 75 seconds

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

Related Documentation

- *Examples: Configuring MSDP*
- [keep-alive \(Protocols MSDP\) on page 273](#)
- [sa-hold-time \(Protocols MSDP\) on page 281](#)

import (Protocols MSDP)

Syntax	<code>import [<i>policy-names</i>];</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp peer <i>address</i>],</p> <p>[edit protocols msdp],</p> <p>[edit protocols msdp group <i>group-name</i>],</p> <p>[edit protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit protocols msdp peer <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp peer <i>address</i>]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</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	Apply one or more policies to routes being imported into the routing table from MSDP.
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 MSDP in a Routing Instance</i> • export on page 269

keep-alive (Protocols MSDP)

Syntax	<code>keep-alive seconds;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols msdp], [edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i> peer address], [edit logical-systems <i>logical-system-name</i> protocols msdp peer address], [edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols msdp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols msdp group <i>group-name</i> peer address], [edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols msdp peer address], [edit protocols msdp], [edit protocols msdp group <i>group-name</i> peer address], [edit protocols msdp peer address], [edit routing-instances <i>instance-name</i> protocols msdp], [edit routing-instances <i>instance-name</i> protocols msdp group <i>group-name</i> peer address] [edit routing-instances <i>instance-name</i> protocols msdp peer address],</p>
Release Information	Statement introduced in Junos OS Release 12.3.
Description	<p>Specify the keepalive interval to use when maintaining a connection with the MSDP peer. If a keepalive message is not received for the hold-time period, the MSDP peer connection is terminated. According to the RFC 3618, <i>Multicast Source Discovery Protocol (MSDP)</i>, the recommended value for the keepalive timer is 60 seconds.</p> <p>The hold-time period must be longer than the keepalive interval.</p> <p>You might want to change the keepalive interval and hold-time period for consistency in a multi-vendor environment.</p>
Default	In Junos OS, the default hold-time period is 75 seconds, and the default keepalive interval is 60 seconds.
Options	<p>seconds—Keepalive interval.</p> <p>Range: 10 through 60 seconds</p> <p>Default: 60 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>Examples: Configuring MSDP</i> • hold-time (Protocols MSDP) on page 271 • sa-hold-time (Protocols MSDP) on page 281

local-address (Protocols MSDP)

Syntax	<code>local-address address;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp peer <i>address</i>],</p> <p>[edit protocols msdp],</p> <p>[edit protocols msdp group <i>group-name</i>],</p> <p>[edit protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit protocols msdp peer <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp peer <i>address</i>]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</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	Configure the local end of an MSDP session. You must configure at least one peer for MSDP to function. When configuring a peer, you must include this statement. This address is used to accept incoming connections to the peer and to establish connections to the remote peer.
Options	address —IP address of the local end of the connection.
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 MSDP in a Routing Instance</i>

log-interval (Protocols MSDP)

Syntax	log-interval <i>seconds</i> ;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols msdp active-source-limit], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp active-source-limit], [edit protocols msdp active-source-limit], [edit routing-instances <i>routing-instance-name</i> protocols msdp active-source-limit]
Release Information	Statement introduced in Junos OS Release 12.2
Description	<p>Specify the minimum time interval (in seconds) between sending consecutive log messages to the system log for MSDP active source messages. To configure the time interval, you must specify the maximum number of MSDP active source messages received by the device.</p> <p>To confirm the configured log interval, use the show msdp source-active command.</p>
Options	<p>seconds—Minimum time interval (in seconds) between log messages. You must explicitly configure the maximum value to configure a time interval to send log messages.</p> <p>Range: 6 through 32,767 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>Example: Configuring MSDP with Active Source Limits and Mesh Groups</i> • log-warning • maximum on page 277

log-warning (Protocols MSDP)

Syntax	log-warning <i>value</i> ;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols msdp active-source-limit], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp active-source-limit], [edit protocols msdp active-source-limit], [edit routing-instances <i>routing-instance-name</i> protocols msdp active-source-limit]
Release Information	Statement introduced in Junos OS Release 12.2
Description	<p>Specify the threshold at which the device logs a warning message in the system log for received MSDP active source messages. This threshold is a percentage of the maximum number of MSDP active source messages received by the device.</p> <p>To confirm the configured warning threshold, use the show msdp source-active command.</p>
Options	<p>value—Percentage of the number of active source messages that starts triggering the warnings. You must explicitly configure the maximum value to configure a warning threshold value.</p> <p>Range: 1 through 100</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 MSDP with Active Source Limits and Mesh Groups</i>• log-interval• maximum on page 277

maximum (MSDP Active Source Messages)

Syntax	<code>maximum <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols msdp active-source-limit], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp active-source-limit], [edit protocols msdp active-source-limit], [edit routing-instances <i>routing-instance-name</i> protocols msdp active-source-limit]
Release Information	Statement introduced before Junos OS Release 7.4. 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	Configure the maximum number of MSDP active source messages the router accepts.
Options	<i>number</i> —Maximum number of active source messages. Range: 1 through 1,000,000 Default: 25,000
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 MSDP with Active Source Limits and Mesh Groups</i> • threshold (MSDP Active Source Messages) on page 283

mode (Protocols MSDP)

Syntax	mode (mesh-group standard);
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>], [edit protocols msdp group <i>group-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. 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	Configure groups of peers in a full mesh topology to limit excessive flooding of source-active messages to neighboring peers. The default flooding mode is standard .
Default	If you do not include this statement, default flooding is applied.
Options	mesh-group —Group of peers that are mesh group members. standard —Use standard MSDP source-active flooding rules. Default: standard
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 MSDP with Active Source Limits and Mesh Groups</i>

peer (Protocols MSDP)

Syntax	<pre> peer address { disable; active-source-limit { maximum number; threshold number; } authentication-key peer-key; default-peer; export [policy-names]; import [policy-names]; local-address address; traceoptions { file filename <files number> <size size> <world-readable no-world-readable>; flag flag <flag-modifier> <disable>; } } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit protocols msdp],</p> <p>[edit protocols msdp group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</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>Define an MSDP peering relationship. An MSDP routing device must know which routing devices are its peers. You define the peer relationships explicitly by configuring the neighboring routing devices that are the MSDP peers of the local routing device. After peer relationships are established, the MSDP peers exchange messages to advertise active multicast sources. To configure multiple MSDP peers, include multiple peer statements.</p> <p>By default, the peer's options are identical to the global or group-level MSDP options. To override the global or group-level options, include peer-specific options within the peer (Protocols MSDP) statement.</p> <p>At least one peer must be configured for MSDP to function. You must configure address and local-address.</p>
Options	<p>address—Name of the MSDP peer.</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

- *Example: Configuring MSDP in a Routing Instance*

rib-group (Protocols MSDP)

Syntax `rib-group group-name;`

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

Release Information Statement introduced before Junos OS Release 7.4.
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 Associate a routing table group with MSDP.

Options *group-name*—Name of the routing table group. 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

- *Example: Configuring MSDP in a Routing Instance*

sa-hold-time (Protocols MSDP)

Syntax	<code>sa-hold-time seconds;</code>
Hierarchy Level	<pre>[edit logical-systems <i>logical-system-name</i> protocols msdp], [edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i> peer address], [edit logical-systems <i>logical-system-name</i> protocols msdp peer address], [edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols msdp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols msdp group <i>group-name</i> peer address], [edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols msdp peer address], [edit protocols msdp], [edit protocols msdp group <i>group-name</i> peer address], [edit protocols msdp peer address], [edit routing-instances <i>instance-name</i> protocols msdp], [edit routing-instances <i>instance-name</i> protocols msdp group <i>group-name</i> peer address] [edit routing-instances <i>instance-name</i> protocols msdp peer address],</pre>
Release Information	Statement introduced in Junos OS Release 12.3.
Description	<p>Specify the source address (SA) message hold time to use when maintaining a connection with the MSDP peer. Each entry in an SA cache has an associated hold time. The hold timer is started when an SA message is received by an MSDP peer. The timer is reset when another SA message is received before the timer expires. If another SA message is not received during the SA message hold-time period, the SA message is removed from the cache.</p> <p>You might want to change the SA message hold time for consistency in a multi-vendor environment.</p>
Options	<p>seconds—Source address message hold time.</p> <p>Range: 75 through 300 seconds</p> <p>Default: 75 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>Examples: Configuring MSDP</i> • hold-time (Protocols MSDP) on page 271 • keep-alive (Protocols MSDP) on page 273

source (Protocols MSDP)

Syntax	<pre>source ip-address </prefix-length> { active-source-limit { maximum number; threshold number; } }</pre>
Hierarchy Level	<pre>[edit logical-systems logical-system-name protocols msdp], [edit logical-systems logical-system-name routing-instances routing-instance-name protocols msdp], [edit protocols msdp], [edit routing-instances routing-instance-name protocols msdp]</pre>
Release Information	Statement introduced before Junos OS Release 7.4. 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	Limit the number of active source messages the routing device accepts from sources in this address range.
Default	If you do not include this statement, the routing device accepts any number of MSDP active source messages.
Options	The other 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>Example: Configuring MSDP with Active Source Limits and Mesh Groups</i>

threshold (MSDP Active Source Messages)

Syntax	<code>threshold <i>number</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols msdp active-source-limit],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp active-source-limit],</p> <p>[edit protocols msdp active-source-limit],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp active-source-limit]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</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 the random early detection (RED) threshold for MSDP active source messages. This number must be less than the configured or default maximum.</p>
Options	<p><i>number</i>—RED threshold for active source messages.</p> <p>Range: 1 through 1,000,000</p> <p>Default: 24,000</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 MSDP with Active Source Limits and Mesh Groups</i> • maximum (MSDP Active Source Messages) on page 277

traceoptions (Protocols MSDP)

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	<p>[edit logical-systems <i>logical-system-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols msdp peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols msdp peer <i>address</i>],</p> <p>[edit protocols msdp],</p> <p>[edit protocols msdp group <i>group-name</i>],</p> <p>[edit protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit protocols msdp peer <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp group <i>group-name</i> peer <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols msdp peer <i>address</i>]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</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 MSDP tracing options.</p> <p>To specify more than one tracing operation, include multiple flag statements.</p>
Default	<p>The default MSDP trace options are those inherited from the routing protocol's traceoptions statement included at the [edit routing-options] hierarchy level.</p>
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 msdp-log file.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named <i>trace-file</i> reaches its maximum size, it is renamed <i>trace-file.0</i>, then <i>trace-file.1</i>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p>

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

Range: 2 through 1000 files

Default: 2 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements.

MSDP Tracing Flags

- **keepalive**—Keepalive messages
- **packets**—All MSDP packets
- **route**—MSDP changes to the routing table
- **source-active**—Source-active packets
- **source-active-request**—Source-active request packets
- **source-active-response**—Source-active response packets

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 any user to read the log file.

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

Default: If you do not include this option, tracing output is appended to an existing trace file.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When **trace-file** again reaches this size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

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

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

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

Default: 1 MB

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

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

Configuration Statements: PIM

- [\[edit protocols pim\] Hierarchy Level on page 290](#)
- [accept-remote-source on page 294](#)
- [address \(Anycast RPs\) on page 295](#)
- [address \(Bidirectional Rendezvous Points\) on page 296](#)
- [address \(Local RPs\) on page 297](#)
- [address \(Static RPs\) on page 298](#)
- [algorithm on page 299](#)
- [anycast-pim on page 300](#)
- [assert-timeout on page 301](#)
- [authentication \(Protocols PIM\) on page 302](#)
- [auto-rp on page 303](#)
- [backoff-period on page 304](#)
- [bfd-liveness-detection \(Protocols PIM\) on page 305](#)
- [bidirectional \(Interface\) on page 306](#)
- [bidirectional \(RP\) on page 307](#)
- [bootstrap on page 308](#)
- [bootstrap-export on page 309](#)
- [bootstrap-import on page 310](#)
- [bootstrap-priority on page 311](#)
- [dense-groups on page 312](#)
- [detection-time \(BFD for PIM\) on page 313](#)
- [df-election on page 314](#)
- [disable \(PIM Graceful Restart\) on page 315](#)
- [disable \(PIM\) on page 316](#)
- [dr-election-on-p2p on page 317](#)
- [dr-register-policy on page 317](#)
- [embedded-rp on page 318](#)
- [export \(Protocols PIM Bootstrap\) on page 319](#)

- [export \(Protocols PIM\) on page 320](#)
- [family \(Bootstrap\) on page 321](#)
- [family \(Protocols PIM\) on page 322](#)
- [family \(Protocols PIM Interface\) on page 323](#)
- [family \(Local RP\) on page 324](#)
- [graceful-restart \(Protocols PIM\) on page 325](#)
- [group \(RPF Selection\) on page 326](#)
- [group-ranges on page 327](#)
- [group-rp-mapping on page 328](#)
- [hello-interval \(Protocols PIM\) on page 329](#)
- [hold-time \(Protocols PIM\) on page 330](#)
- [idle-standby-path-switchover-delay on page 331](#)
- [import \(Protocols PIM Bootstrap\) on page 332](#)
- [import \(Protocols PIM\) on page 333](#)
- [infinity on page 334](#)
- [interface \(Protocols PIM\) on page 335](#)
- [join-load-balance on page 337](#)
- [join-prune-timeout on page 338](#)
- [key-chain \(Protocols PIM\) on page 339](#)
- [local on page 340](#)
- [local-address \(Protocols PIM\) on page 341](#)
- [log-interval \(PIM Entries\) on page 342](#)
- [loose-check on page 343](#)
- [mapping-agent-election on page 344](#)
- [maximum \(PIM Entries\) on page 345](#)
- [maximum-rps on page 346](#)
- [minimum-interval \(PIM BFD Liveness Detection\) on page 347](#)
- [minimum-interval \(PIM BFD Transmit Interval\) on page 348](#)
- [minimum-receive-interval on page 349](#)
- [mode \(Protocols PIM\) on page 350](#)
- [multiplier on page 351](#)
- [neighbor-policy on page 351](#)
- [next-hop \(PIM RPF Selection\) on page 352](#)
- [no-adaptation \(PIM BFD Liveness Detection\) on page 352](#)
- [no-bidirectional-mode on page 353](#)
- [no-dr-flood \(PIM Snooping\) on page 354](#)
- [offer-period on page 355](#)

- [override \(PIM static RP\) on page 356](#)
- [override-interval on page 357](#)
- [pim on page 358](#)
- [pim-snooping on page 363](#)
- [prefix-list \(PIM RPF Selection\) on page 364](#)
- [priority \(Bootstrap\) on page 365](#)
- [priority \(PIM Interfaces\) on page 366](#)
- [priority \(PIM RPs\) on page 367](#)
- [propagation-delay on page 368](#)
- [register-limit on page 369](#)
- [reset-tracking-bit on page 370](#)
- [restart-duration \(Protocols PIM\) on page 371](#)
- [rib-group \(Protocols PIM\) on page 372](#)
- [robustness-count on page 373](#)
- [rp on page 374](#)
- [rp-register-policy on page 376](#)
- [rp-set on page 377](#)
- [rpf-selection on page 378](#)
- [sglimit on page 379](#)
- [source \(PIM RPF Selection\) on page 380](#)
- [spt-threshold on page 381](#)
- [standby-path-creation-delay on page 382](#)
- [static \(Protocols PIM\) on page 383](#)
- [threshold \(PIM BFD Detection Time\) on page 384](#)
- [threshold \(PIM BFD Transmit Interval\) on page 385](#)
- [threshold \(PIM Entries\) on page 386](#)
- [traceoptions \(Protocols PIM\) on page 388](#)
- [traceoptions \(PIM Snooping\) on page 391](#)
- [transmit-interval \(PIM BFD Liveness Detection\) on page 392](#)
- [tunnel-devices \(Tunnel-Capable PICs\) on page 393](#)
- [version \(BFD\) on page 394](#)
- [version \(PIM\) on page 395](#)
- [vlan \(PIM Snooping\) on page 396](#)
- [vpn-group-address on page 396](#)
- [wildcard-source \(PIM RPF Selection\) on page 397](#)

[edit protocols pim] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  pim {
    disable;
    assert-timeout seconds;
    default-vpn-source {
      interface-name interface-name;
    }
    dense-groups {
      address <announce | reject>;
    }
    dr-election-on-p2p;
    export [ policy-names ];
    family (inet | inet6) {
      disable;
    }
    graceful-restart {
      disable;
      no-bidirectional-mode;
      restart-duration seconds;
    }
    import [ policy-names ];
    interface interface-name {
      ... the interface subhierarchy appears after the main [edit protocols pim] hierarchy ...
      family (inet | inet6) {
        disable;
      }
    }
    join-load-balance;
    join-prune-timeout seconds;
    nonstop-routing {
      disable;
    }
    override-interval milliseconds;
    propagation-delay milliseconds;
    reset-tracking-bit;
    rib-group {
      inet group-name;
      inet6 group-name;
    }
    rp {
      ... the rp subhierarchy appears after the main [edit protocols pim] hierarchy ...
    }
    sglimit {
      family (inet | inet6) {
        log-interval seconds;
        maximum limit;
        threshold value;
      }
    }
  }
}

```

```

    log-interval seconds;
    maximum limit;
    threshold value;
  }
}
spt-threshold {
  infinity [ policy-names ];
}
traceoptions {
  file filename <files number> <size maximum-file-size> <world-readable |
    no-world-readable>;
  flag flag <flag-modifier> <disable>;
  flag (route | state) <flag-modifier> <disable> <filter <match-on prefix>
    <policy [ policy-names ]>>;
}
}

pim {
  interface interface-name {
    accept-remote-source;
    disable;
    bfd-liveness-detection {
      authentication {
        algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
          meticulous-keyed-sha-1 | simple-password);
        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 (1 | automatic);
    }
    bidirectional {
      df-election {
        backoff-period milliseconds;
        offer-period milliseconds;
        robustness-count number;
      }
    }
  }
  family (inet | inet6) {
    disable;
  }
  hello-interval seconds;
  bidirectional-sparse | bidirectional-sparse-dense 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 (1 | 2);
  }
}

pim {
  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-export [ policy-names ];
    bootstrap-import [ policy-names ];
    bootstrap-priority number;
    dr-register-policy [ policy-names ];
    embedded-rp {
      group-ranges {
        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 {
  ... the local subhierarchy appears after the main [edit protocols pim rp] hierarchy ...
}

register-limit {
  family (inet | inet6) {

```

```

        log-interval seconds;
        maximum limit;
        threshold value;
    }
}
log-interval seconds;
maximum limit;
threshold value;
}
}
rp-register-policy [ policy-names ];
static {
    address address {
        group-ranges {
            ip-prefix </prefix-length>;
        }
        override;
        version (1 | 2);
    }
}
}

rp {
    local {
        disable;
        address address;
        family (inet | inet6) {
            disable;
            address address;
            anycast-pim {
                local-address address;
                rp-set {
                    address address <forward-msdp-sa>;
                }
            }
            group-ranges {
                ip-prefix </prefix-length>;
            }
            hold-time seconds;
            override;
            priority number;
        }
        group-ranges {
            ip-prefix </prefix-length>;
        }
        hold-time seconds;
        override;
        priority number;
    }
}
}
}

```

- Related Documentation**
- *Notational Conventions Used in Junos OS Configuration Hierarchies*
 - *[edit protocols] Hierarchy Level*

accept-remote-source

Syntax	accept-remote-source;
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 in Junos OS Release 9.6. Statement introduced in Junos OS Release 9.6 for EX Series switches. Statement introduced in Junos OS Release 13.2R2 for PTX Series routers but is not supported for services requiring tunnel-services.
Description	Accept traffic from a remote source. A remote source is a source that is not on the same subnet as the incoming interface. This statement enables the remote source to be learned and advertised by MSDP so that receivers in other MSDP areas can join the source. You do not need to disable RPF checking, but you do need to ensure that the best path to reach the remote source is through the incoming 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>Configuring the Interface to Accept Traffic from a Remote Source</i>• <i>Example: Allowing MBGP MVPN Remote Sources</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 pim rp local (inet inet6) anycast-pim rp-set],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp local (inet inet6) anycast-pim rp-set],</p> <p>[edit protocols pim rp local (inet inet6) anycast-pim rp-set],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp local (inet inet6) anycast-pim rp-set]</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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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 (Bidirectional Rendezvous Points)

Syntax	<pre>address address { group-ranges { destination-ip-prefix </prefix-length>; } hold-time seconds; priority number; }</pre>
Hierarchy Level	<pre>[edit logical-systems <i>logical-system-name</i> protocols pim rp bidirectional], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp bidirectional], [edit protocols pim rp bidirectional], [edit routing-instances <i>routing-instance-name</i> protocols pim rp bidirectional]</pre>
Release Information	<p>Statement introduced in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 13.3 for the PTX5000 router.</p>
Description	<p>Configure bidirectional rendezvous point (RP) addresses. The address can be a loopback interface address, an address of a link interface, or an address that is not assigned to an interface but belongs to a subnet that is reachable by the bidirectional PIM routing devices in the network.</p>
Options	<p>address—Bidirectional RP address.</p> <p>Default: 232.0.0.0/8</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>Understanding Bidirectional PIM</i>• <i>Example: Configuring Bidirectional PIM</i>

address (Local RPs)

Syntax	<code>address <i>address</i>;</code>
Hierarchy Level	<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 rp local family (inet inet6)],</p> <p>[edit protocols pim rp local family (inet inet6)],</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>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Configure the local rendezvous point (RP) address.
Options	<i>address</i> —Local RP address.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Local PIM RPs on page 107

address (Static RPs)

Syntax	<pre>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 static], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp static], [edit protocols pim static], [edit routing-instances <i>routing-instance-name</i> protocols pim rp 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 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	<p>Configure static rendezvous point (RP) addresses. 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>
Options	<p>address—Static RP address.</p> <p>Default: 224.0.0.0/4</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 on page 111

algorithm

Syntax	<code>algorithm <i>algorithm-name</i>;</code>
Hierarchy Level	[edit protocols pim interface <i>interface-name</i> bfd-liveness-detection authentication], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> bfd-liveness-detection authentication]
Release Information	Statement introduced in Junos OS Release 9.6. 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 algorithm to use for BFD authentication.
Options	<p><i>algorithm-name</i>—Name of algorithm to use for BFD authentication:</p> <ul style="list-style-type: none"> • simple-password—Plain-text password. One to 16 bytes of plain text. One or more passwords can be configured. • keyed-md5—Keyed Message Digest 5 hash algorithm for sessions with transmit and receive rates greater than 100 ms. • meticulous-keyed-md5—Meticulous keyed Message Digest 5 hash algorithm. • keyed-sha-1—Keyed Secure Hash Algorithm I for sessions with transmit and receive rates greater than 100 ms. • meticulous-keyed-sha-1—Meticulous keyed Secure Hash Algorithm I.
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"> • Understanding Bidirectional Forwarding Detection Authentication for PIM on page 131 • Configuring BFD Authentication for PIM on page 134 • authentication on page 302

anycast-pim

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

assert-timeout

Syntax	<code>assert-timeout <i>seconds</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	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	<i>seconds</i> —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>

authentication (Protocols PIM)

Syntax	<pre>authentication { algorithm <i>algorithm-name</i>; key-chain <i>key-chain-name</i>; loose-check; }</pre>
Hierarchy Level	[edit protocols pim interface <i>interface-name</i> family (inet inet6) bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols pim interface family (inet inet6) <i>interface-name</i> bfd-liveness-detection]
Release Information	Statement introduced in Junos OS Release 9.6. 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	Configure the algorithm, security keychain, and level of authentication for BFD sessions running on PIM interfaces. The remaining statements are explained separately.
Options	The 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 BFD Authentication for PIM on page 134• Configuring BFD for PIM on page 133• Understanding Bidirectional Forwarding Detection Authentication for PIM on page 131• bfd-liveness-detection on page 305• key-chain (Protocols PIM) on page 339• loose-check on page 343

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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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"> • Configuring PIM Auto-RP on page 99

backoff-period

Syntax	<code>backoff-period <i>milliseconds</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols <code>pim interface interface-name</code> bidirectional df-election], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols <code>pim interface interface-name</code> bidirectional df-election], [edit protocols <code>pim interface interface-name</code> bidirectional df-election], [edit routing-instances <i>routing-instance-name</i> protocols <code>pim interface interface-name</code> bidirectional df-election]
Release Information	Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 13.3 for the PTX5000 router.
Description	Configure the designated forwarder (DF) election backoff period for bidirectional PIM. The backoff-period statement configures the period that the acting DF waits between receiving a better DF Offer and sending the Pass message to transfer DF responsibility.



NOTE: Junos OS checks rendezvous point (RP) unicast reachability before accepting incoming DF messages. DF messages for unreachable rendezvous points are ignored. This is needed to prevent the following example scenario. Routers A and B are downstream routing devices on the same LAN, and both are supposed to send DF election messages with an infinite metric on their upstream interfaces (reverse-path forwarding [RPF] interfaces). Router A has a higher IP address than Router B. When both routing devices lose the path to the RP, both send an Offer message with the infinite metric onto the LAN. Router A wins the election because it has a higher IP address, and Router B backs off as a result. After three Offer messages, according to RFC 5015, Router A looks up the RP and finds no path to the RP. As a result, Router A transitions to the Lose state and sends nothing. On the other hand, after backing off for an interval of 3 x the Offer period, Router B does not receive any messages, and resumes the DF election by sending a new Offer message. Hence, the pattern repeats indefinitely.

Options	<i>milliseconds</i> —Period that the acting DF waits between receiving a better DF Offer and sending the Pass message to transfer DF responsibility. Range: 100 through 65,535 milliseconds Default: 1000
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>Understanding Bidirectional PIM</i> • <i>Example: Configuring Bidirectional PIM</i>

bfd-liveness-detection (Protocols PIM)

Syntax	<pre> bfd-liveness-detection { authentication { algorithm <i>algorithm-name</i>; key-chain <i>key-chain-name</i>; loose-check; } detection-time { threshold <i>milliseconds</i>; } minimum-interval <i>milliseconds</i>; minimum-receive-interval <i>milliseconds</i>; multiplier <i>number</i>; no-adaptation; transmit-interval { minimum-interval <i>milliseconds</i>; threshold <i>milliseconds</i>; } version (0 1 automatic); } </pre>
Hierarchy Level	<p>[edit protocols pim interface <i>interface-name</i> family (inet inet6)], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> family (inet inet6)]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.1. authentication option introduced in Junos OS Release 9.6. 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.</p>
Description	<p>Configure bidirectional forwarding detection (BFD) timers and authentication for 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"> • Configuring BFD for PIM on page 133 • Configuring BFD Authentication for PIM on page 134

bidirectional (Interface)

Syntax	<pre>bidirectional { df-election { backoff-period milliseconds; offer-period milliseconds; robustness-count number; } }</pre>
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 12.1. Statement introduced in Junos OS Release 13.3 for the PTX5000 router.
Description	Configure parameters for bidirectional PIM. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Understanding Bidirectional PIM</i>• <i>Example: Configuring Bidirectional PIM</i>

bidirectional (RP)

Syntax	<pre> bidirectional { address address { group-ranges { destination-ip-prefix</prefix-length>; } hold-time seconds; priority number; } } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp], [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]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 13.3 for the PTX5000 router.</p>
Description	<p>Configure the routing device's rendezvous-point (RP) properties for bidirectional 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>Understanding Bidirectional PIM</i> • <i>Example: Configuring Bidirectional PIM</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	<pre>[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]</pre>
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	<p>Configure parameters to control bootstrap routers and messages.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring PIM Bootstrap Properties for IPv4 on page 113• Configuring PIM Bootstrap Properties for IPv4 or IPv6 on page 114

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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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"> • Configuring PIM Bootstrap Properties for IPv4 on page 113 • Configuring PIM Bootstrap Properties for IPv4 or IPv6 on page 114 • bootstrap-import on page 310

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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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">• Configuring PIM Bootstrap Properties for IPv4 on page 113• Configuring PIM Bootstrap Properties for IPv4 or IPv6 on page 114• bootstrap-export on page 309

bootstrap-priority

Syntax	<code>bootstrap-priority <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp], [edit protocols pim rp], [edit routing-instances <i>routing-instance-name</i> protocols pim rp]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. 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 whether this routing device is eligible to be a bootstrap router. In the case of a tie, the routing device with the highest IP address is elected to be the bootstrap router.
Options	<i>number</i> —Priority for becoming the bootstrap router. A value of 0 means that the routing device is not eligible to be the bootstrap router. Range: 0 through 255 Default: 0
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring PIM Bootstrap Properties for IPv4 on page 113

dense-groups

Syntax	<code>dense-groups { <i>addresses</i>; }</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. 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 which groups are operating in dense mode.
Options	<i>addresses</i> —Address of groups operating in dense mode.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring PIM Sparse-Dense Mode Properties on page 97

detection-time (BFD for PIM)

Syntax	<pre> detection-time { threshold milliseconds; } </pre>
Hierarchy Level	[edit protocols pim interface <i>interface-name</i> bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> bfd-liveness-detection]
Release Information	<p>Statement introduced in Junos OS Release 8.2.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for BFD authentication introduced in Junos OS Release 9.6.</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>Enable BFD failure detection. The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. The lower the BFD failure detection timer value, the faster the failure detection and vice versa. For example, the timers can adapt to a higher value if the adjacency fails (that is, the timer detects failures more slowly). Or a neighbor can negotiate a higher value for a timer than the configured value. The timers adapt to a higher value when a BFD session flap occurs more than three times in a span of 15 seconds. A back-off algorithm increases the receive (Rx) interval by two if the local BFD instance is the reason for the session flap. The transmission (Tx) interval is increased by two if the remote BFD instance is the reason for the session flap. You can use the clear bfd adaptation command to return BFD interval timers to their configured values. The clear bfd adaptation command is hitless, meaning that the command does not affect traffic flow on the routing device.</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"> • Configuring BFD for PIM on page 133 • bfd-liveness-detection on page 305 • threshold on page 384

df-election

Syntax	<pre>df-election { backoff-period <i>milliseconds</i>; offer-period <i>milliseconds</i>; robustness-count <i>number</i>; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim interface <i>interface-name</i> bidirectional], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> bidirectional], [edit protocols pim interface <i>interface-name</i> bidirectional], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> bidirectional]
Release Information	Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 13.3 for the PTX5000 router.
Description	Optionally, configure the designated forwarder (DF) election parameters for bidirectional PIM. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Understanding Bidirectional PIM</i>• <i>Example: Configuring Bidirectional PIM</i>

disable (PIM Graceful Restart)

Syntax	disable;
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	Explicitly disable PIM sparse mode graceful restart.
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>

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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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 on page 84 disable (PIM Graceful Restart) on page 315

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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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"> • Configuring PIM Designated Router Election on Point-to-Point Links on page 91

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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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"> • Configuring Register Message Filters on a PIM RP and DR on page 128 • rp-register-policy on page 376

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], [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]</p>
Release Information	<p>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.</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. routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring PIM Embedded RP for IPv6 on page 105

export (Protocols PIM Bootstrap)

Syntax	<code>export [<i>policy-names</i>];</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp bootstrap family (inet inet6)],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap family (inet inet6)],</p> <p>[edit protocols pim rp bootstrap family (inet inet6)],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap family (inet inet6)]</p>
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <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 export policies to control outgoing PIM bootstrap messages.
Options	<i>policy-names</i> —Name of one or more import policies.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring PIM Bootstrap Properties for IPv4 on page 113 • Configuring PIM Bootstrap Properties for IPv4 or IPv6 on page 114 • import (Protocols PIM Bootstrap) on page 332

export (Protocols PIM)

Syntax	<code>export [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim]
Release Information	Statement introduced in Junos OS Release 9.6. 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 join and prune messages. PIM join and prune filters can be applied to PIM-SM and PIM-SSM messages. PIM join and prune filters cannot be applied to PIM-DM messages.
Required Privilege Level	view-level—To view this statement in the configuration. control-level—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Filtering Outgoing PIM Join Messages on page 121

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> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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"> • Configuring PIM Bootstrap Properties for IPv4 on page 113 • Configuring PIM Bootstrap Properties for IPv4 or IPv6 on page 114

family (Protocols PIM)

Syntax	family (inet inet6) { disable; }
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], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6. Statement introduced in Junos OS 11.3 for the QFX Series.
Description	Enable the PIM protocol for the specified family.
Options	inet —Enable the PIM protocol for the IP version 4 (IPv4) address family. inet6 —Enable the PIM protocol for the IP version 6 (IPv6) address family. The remaining statement is explained separately.
Related Documentation	<ul style="list-style-type: none">• Disabling PIM on page 84• disable (PIM Graceful Restart) on page 315• disable (PIM) on page 316

family (Protocols PIM Interface)

Syntax	<pre> family (inet inet6) { bfd-liveness-detection { authentication { algorithm <i>algorithm-name</i>; key-chain <i>key-chain-name</i>; loose-check; } detection-time { threshold <i>milliseconds</i>; } minimum-interval <i>milliseconds</i>; minimum-receive-interval <i>milliseconds</i>; multiplier <i>number</i>; no-adaptation; transmit-interval { minimum-interval <i>milliseconds</i>; threshold <i>milliseconds</i>; } version (0 1 automatic); } disable; } </pre>
Hierarchy Level	<p>[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]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Support for the Bidirectional Forwarding Detection (BFD) Protocol statements was introduced in Junos OS Release 12.2.</p>
Description	<p>Configure one of the following PIM protocol settings for the specified family on the specified interface:</p> <ul style="list-style-type: none"> • BFD protocol settings • Disable PIM
Options	<p>inet—Enable the PIM protocol for the IP version 4 (IPv4) address family.</p> <p>inet6—Enable the PIM protocol for the IP version 6 (IPv6) address family.</p> <p>The remaining statements are explained separately.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring PIM and the Bidirectional Forwarding Detection (BFD) Protocol on page 131 • Disabling PIM on page 84

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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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">• Configuring Local PIM RPs on page 107

graceful-restart (Protocols PIM)

Syntax	<pre>graceful-restart { disable; no-bidirectional-mode; restart-duration seconds; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim],</p> <p>[edit protocols pim],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p>
Description	<p>Configure PIM sparse mode graceful restart.</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 Sparse Mode Graceful Restart</i>


group (RPF Selection)

Syntax	<pre>group group-address{ source source-address{ next-hop next-hop-address; } wildcard-source { next-hop next-hop-address; } }</pre>
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> edit protocols pim rpf-selection]
Release Information	Statement introduced in JUNOS Release 10.4. 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 PIM group address for which you configure RPF selection group (RPF Selection) .
Default	By default, PIM RPF selection is not configured.
Options	group-address —PIM group address for which you configure RPF selection.
Required Privilege Level	view-level—To view this statement in the configuration. control-level—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring PIM RPF Selection</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"> • Configuring Local PIM RPs on page 107 • Configuring PIM Embedded RP for IPv6 on page 105 • Example: Configuring Bidirectional PIM

group-rp-mapping

Syntax	<pre>group-rp-mapping { family (inet inet6) { log-interval seconds; maximum limit; threshold value; } log-interval seconds; maximum limit; threshold value; }</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	Statement introduced in Junos OS Release 12.2.
Description	Configure a limit for the number of incoming group-to-RP mappings.
<div>  <p>NOTE: The maximum limit settings that you configure with the maximum and the family (inet inet6) maximum statements are mutually exclusive. For example, if you configure a global maximum group-to-RP mapping limit, you cannot configure a limit at the family level for IPv4 or IPv6. If you attempt to configure a limit at both the global level and the family level, the device will not accept the configuration.</p> </div>	
Options	<p>family (inet inet6)—(Optional) Specify either IPv4 or IPv6 messages to be counted towards the configured group-to-RP mapping limit.</p> <p>Default: Both IPv4 and IPv6 messages are counted towards the configured group-to-RP limit.</p> <p>The remaining statements are described 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 State Limits</i>

hello-interval (Protocols PIM)

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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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 on page 330 • Modifying the PIM Hello Interval on page 80

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>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	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: 0 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"> • Configuring Local PIM RPs on page 107 in the <i>Multicast Protocols Feature Guide for Routing Devices</i> • <i>Example: Configuring Bidirectional PIM</i>

idle-standby-path-switchover-delay

Syntax	<code>idle-standby-path-switchover-delay <seconds>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim],</p> <p>[edit protocols pim],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim]</p>
Release Information	Statement introduced in Junos OS Release 12.2.
Description	<p>Configure the time interval after which an ECMP join is moved to the standby path in the absence of traffic on the path.</p> <p>In the absence of this statement, ECMP joins are not moved to the standby path until traffic is detected on the path.</p>
Options	<code><seconds></code> —Time interval after which an ECMP join is moved to the standby RPF path in the absence of traffic on the path.
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 Make-Before-Break Join Load Balancing</i> • <i>Configuring PIM Join Load Balancing</i> • clear pim join-distribution on page 508 • join-load-balance on page 337 • standby-path-creation-delay on page 382

import (Protocols PIM Bootstrap)

Syntax	<code>import [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols pim rp bootstrap (inet inet6)], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap (inet inet6)], [edit protocols pim rp bootstrap (inet inet6)], [edit routing-instances <i>routing-instance-name</i> protocols pim rp bootstrap (inet inet6)]
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 9.0 for EX Series switches. 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 import policies to control incoming PIM bootstrap messages.
Options	<i>policy-names</i> —Name of one or more import policies.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring PIM Bootstrap Properties for IPv4 on page 113• Configuring PIM Bootstrap Properties for IPv4 or IPv6 on page 114• export (Protocols PIM Bootstrap) on page 319

import (Protocols PIM)

Syntax	<code>import [<i>policy-names</i>];</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim],</p> <p>[edit protocols pim],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <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 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	<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"> • Filtering Incoming PIM Join Messages on page 124

infinity

Syntax	<code>infinity [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols <code>pim spt-threshold</code>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols <code>pim spt-threshold</code>], [edit protocols <code>pim spt-threshold</code>], [edit routing-instances <i>routing-instance-name</i> protocols <code>pim spt-threshold</code>]
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	Apply one or more policies to set the SPT threshold to infinity for a source-group address pair. Use the infinity statement to prevent the last-hop routing device from transitioning from the RPT rooted at the RP to an SPT rooted at the source for that source-group address pair.
Options	<i>policy-names</i> —Name of one or more policies.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring the PIM SPT Threshold Policy</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 on page 82](#)

join-load-balance

Syntax	join-load-balance { automatic; }
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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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>Example: Configuring PIM Make-Before-Break Join Load Balancing</i> • <i>Configuring PIM Join Load Balancing</i> • clear pim join-distribution on page 508 in the CLI Explorer

join-prune-timeout

Syntax	join-prune-timeout <i>seconds</i> ;
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 8.4. 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 timeout for the join state. If the periodic join refresh message is not received before the timeout expires, the join state is removed.
Options	seconds —Number of seconds to wait for the periodic join message to arrive. Range: 210 through 240 seconds Default: 210 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 Join State Timeout</i>

key-chain (Protocols PIM)

Syntax	<code>key-chain <i>key-chain-name</i>;</code>
Hierarchy Level	<p>[edit protocols pim interface <i>interface-name</i> family {inet inet6} bfd-liveness-detection authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> family {inet inet6} bfd-liveness-detection authentication]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Statement modified in Junos OS Release 12.2 to include family in the hierarchy level.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Specify the security keychain to use for BFD authentication.
Options	<p><i>key-chain-name</i>—Name of the security keychain to use for BFD authentication. The name is a unique integer between 0 and 63. This must match one of the keychains in the authentication-key-chains statement at the [edit security] hierarchy level.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring BFD Authentication for PIM on page 134 • Understanding Bidirectional Forwarding Detection Authentication for PIM on page 131 • authentication on page 302

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>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Configure the routing device's RP properties.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Local PIM RPs on page 107

local-address (Protocols PIM)

Syntax	<code>local-address address;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp 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 rp local family (inet inet6) anycast-pim],</p> <p>[edit protocols pim rp local family (inet inet6) anycast-pim],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp 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	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	<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>

log-interval (PIM Entries)

Syntax	log-interval <i>value</i> ;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim sglimit],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim sglimit <i>family</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim sglimit],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim sglimit <i>family</i>],</p> <p>[edit protocols pim sglimit],</p> <p>[edit protocols pim sglimit <i>family</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim sglimit],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim sglimit <i>family</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp group-rp-mapping],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp group-rp-mapping <i>family</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp group-rp-mapping],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp group-rp-mapping <i>family</i>],</p> <p>[edit protocols pim rp group-rp-mapping],</p> <p>[edit protocols pim rp group-rp-mapping <i>family</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp group-rp-mapping],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp group-rp-mapping <i>family</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp register-limit],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp register-limit <i>family</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp register-limit],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp register-limit <i>family</i>],</p> <p>[edit protocols pim rp register-limit],</p> <p>[edit protocols pim rp register-limit <i>family</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp register-limit],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp register-limit <i>family</i>],</p>
Release Information	Statement introduced in Junos OS Release 12.2.
Description	Configure the amount of time between log messages.
Options	<p><i>seconds</i>—Minimum time interval (in seconds) between log messages. To configure the time interval, you must explicitly configure the maximum number of entries received with the maximum statement. You can apply the log interval to incoming PIM join messages, PIM register messages, and group-to-RP mappings.</p> <p>Range: 1 through 65,535</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"> add new concept and example topic to related topic list. clear pim join on page 506


loose-check

Syntax	loose-check;
Hierarchy Level	[edit protocols pim interface <i>interface-name</i> bfd-liveness-detection authentication], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> bfd-liveness-detection authentication]
Release Information	Statement introduced in Junos OS Release 9.6. 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	<p>Specify loose authentication checking on the BFD session. Use loose authentication for transitional periods only when authentication might not be configured at both ends of the BFD session.</p> <p>By default, strict authentication is enabled and authentication is checked at both ends of each BFD session. Optionally, to smooth migration from nonauthenticated sessions to authenticated sessions, you can configure <i>loose checking</i>. When loose checking is configured, packets are accepted without authentication being checked at each end of the session.</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 BFD Authentication for PIM on page 134 • Understanding Bidirectional Forwarding Detection Authentication for PIM on page 131 • authentication on page 302

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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the routing device mapping announcements as a mapping agent.
Options	mapping-agent-election —Mapping agents do not announce mappings when receiving mapping messages from a higher-addressed mapping agent. no-mapping-agent-election —Mapping agents always announce mappings and do not perform mapping agent election. Default: mapping-agent-election
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring PIM Auto-RP on page 99

maximum (PIM Entries)

Syntax	<code>maximum <i>limit</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim sglimit],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim sglimit <i>family</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim sglimit],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim sglimit <i>family</i>],</p> <p>[edit protocols pim sglimit],</p> <p>[edit protocols pim sglimit <i>family</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim sglimit],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim sglimit <i>family</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp group-rp-mapping],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp group-rp-mapping <i>family</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp group-rp-mapping],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp group-rp-mapping <i>family</i>],</p> <p>[edit protocols pim rp group-rp-mapping],</p> <p>[edit protocols pim rp group-rp-mapping <i>family</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp group-rp-mapping],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp group-rp-mapping <i>family</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp register-limit],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp register-limit <i>family</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp register-limit],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp register-limit <i>family</i>],</p> <p>[edit protocols pim rp register-limit],</p> <p>[edit protocols pim rp register-limit <i>family</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp register-limit],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp register-limit <i>family</i>],</p>
Release Information	Statement introduced in Junos OS Release 12.2.
Description	Configure the maximum number of specified PIM entries received by the device. If the device reaches the configured limit, no new entries are received.
	<div>  <p>NOTE: The maximum limit settings that you configure with the maximum and the family (inet inet6) maximum statements are mutually exclusive. For example, if you configure a global maximum PIM join state limit, you cannot configure a limit at the family level for IPv4 or IPv6 joins. If you attempt to configure a limit at both the global level and the family level, the device will not accept the configuration.</p> </div>
Options	<p>limit—Maximum number of PIM entries received by the device. If you configure both the log-interval and the maximum statements, a warning is triggered when the maximum limit is reached.</p>

Depending on your configuration, this limit specifies the maximum number of PIM joins, PIM register messages, or group-to-RP mappings received by the device.

Range: 1 through 65,535

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

Related Documentation

- add new concept and example topic to related topic list.
- [clear pim join on page 506](#)

maximum-rps

Syntax maximum-rps *limit*;

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

Description Limit the number of RPs that the routing device acknowledges.

Options *limit*—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

- [Configuring PIM Embedded RP for IPv6 on page 105](#)

minimum-interval (PIM BFD Liveness Detection)

Syntax	<code>minimum-interval <i>milliseconds</i>;</code>
Hierarchy Level	[edit protocols <code>pim interface <i>interface-name</i> bfd-liveness-detection</code>], [edit routing-instances <i>routing-instance-name</i> protocols <code>pim interface <i>interface-name</i> bfd-liveness-detection</code>]
Release Information	Statement introduced in Junos OS Release 8.1. 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	Configure the minimum interval after which the local routing device transmits hello packets and then expects to receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can specify the minimum transmit and receive intervals separately using the <code>transmit-interval</code> <code>minimum-interval</code> and <code>minimum-receive-interval</code> statements.
Options	<i>milliseconds</i> —Minimum transmit and receive interval. Range: 1 through 255,000 milliseconds
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 BFD for PIM on page 133

minimum-interval (PIM BFD Transmit Interval)

Syntax	<code>minimum-interval <i>milliseconds</i>;</code>
Hierarchy Level	[edit protocols pim interface <i>interface-name</i> bfd-liveness-detection transmit-interval], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> bfd-liveness-detection transmit-interval]
Release Information	Statement introduced in Junos OS Release 8.2. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for BFD authentication introduced in Junos OS Release 9.6. 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	Configure the minimum interval after which the local routing device transmits hello packets to a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can configure the minimum transmit interval using the minimum-interval statement at the [edit protocols pim interface <i>interface-name</i> bfd-liveness-detection] hierarchy level.
Options	<i>milliseconds</i> —Minimum transmit interval value. Range: 1 through 255,000
<div style="display: flex; align-items: center;">  <div> <p>NOTE: The threshold value specified in the threshold statement must be greater than the value specified in the minimum-interval statement for the transmit-interval statement.</p> </div> </div>	
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring BFD for PIM on page 133 • bfd-liveness-detection on page 305 • minimum-interval on page 347 • threshold on page 385

minimum-receive-interval

Syntax	<code>minimum-receive-interval <i>milliseconds</i>;</code>
Hierarchy Level	[edit protocols <code>pim interface <i>interface-name</i> bfd-liveness-detection</code>], [edit routing-instances <i>routing-instance-name</i> protocols <code>pim interface <i>interface-name</i> bfd-liveness-detection</code>]
Release Information	Statement introduced in Junos OS Release 8.1. 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	Configure the minimum interval after which the local routing device must receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can configure the minimum receive interval using the <code>minimum-interval</code> statement at the [edit protocols <code>pim interface <i>interface-name</i> bfd-liveness-detection</code>] hierarchy level.
Options	<i>milliseconds</i> —Minimum receive interval. Range: 1 through 255,000 milliseconds
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 BFD for PIM on page 133

mode (Protocols PIM)

Syntax	<code>mode (bidirectional-sparse bidirectional-sparse-dense dense sparse sparse-dense);</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. 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">• Configuring PIM Dense Mode Properties on page 95 in the <i>Multicast Protocols Feature Guide for Routing Devices</i>• Configuring PIM Sparse-Dense Mode Properties on page 97 in the <i>Multicast Protocols Feature Guide for Routing Devices</i>• Example: Configuring Bidirectional PIM

multiplier

Syntax	<code>multiplier <i>number</i>;</code>
Hierarchy Level	[edit protocols <code>pim interface <i>interface-name</i> bfd-liveness-detection</code>], [edit routing-instances <code><i>routing-instance-name</i> protocols pim interface <i>interface-name</i> bfd-liveness-detection</code>]
Release Information	Statement introduced in Junos OS Release 8.1. 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	Configure the number of hello packets not received by a neighbor that causes the originating interface to be declared down.
Options	<i>number</i> —Number of hello packets. Range: 1 through 255 Default: 3
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 BFD for PIM on page 133

neighbor-policy

Syntax	<code>neighbor-policy [<i>policy-names</i>];</code>
Hierarchy Level	[edit logical-systems <code><i>logical-system-name</i> protocols pim interface <i>interface-name</i></code>], [edit logical-systems <code><i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i></code>], [edit protocols <code>pim interface <i>interface-name</i></code>], [edit routing-instances <code><i>routing-instance-name</i> protocols pim interface <i>interface-name</i></code>]
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. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX 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"> • Configuring Interface-Level PIM Neighbor Policies on page 120

next-hop (PIM RPF Selection)

Syntax	<code>next-hop <i>next-hop-address</i>;</code>
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> protocols pim rpf-selection group <i>group-address</i> source <i>source-address</i>], [edit routing-instances <i>routing-instance-name</i> protocols pim rpf-selection group <i>group-address</i> wildcard-source], [edit routing-instances <i>routing-instance-name</i> protocols pim rpf-selection prefix-list <i>prefix-list-addresses</i> source <i>source-address</i>], [edit routing-instances <i>routing-instance-name</i> protocols pim rpf-selection prefix-list <i>prefix-list-addresses</i> wildcard-source]
Release Information	Statement introduced in JUNOS Release 10.4. 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 specific next-hop address for the PIM group source.
Options	<i>next-hop-address</i> —Specific next-hop address for the PIM group source.
Required Privilege Level	view-level—To view this statement in the configuration. control-level—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring PIM RPF Selection

no-adaptation (PIM BFD Liveness Detection)

Syntax	<code>no-adaptation;</code>
Hierarchy Level	[edit protocols pim interface <i>interface-name</i> bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> bfd-liveness-detection]
Release Information	Statement introduced in Junos OS Release 9.0 Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for BFD authentication introduced in Junos OS Release 9.6. 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	Configure BFD sessions not to adapt to changing network conditions. We recommend that you <i>do not</i> disable BFD adaptation unless it is preferable to have BFD adaptation disabled in your network.
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 BFD for PIM on page 133• bfd-liveness-detection on page 305

no-bidirectional-mode

Syntax	no-bidirectional-mode;
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 in Junos OS Release 12.1. Statement introduced in Junos OS Release 13.3 for the PTX5000 router.
Description	<p>Disable forwarding for bidirectional PIM routes during graceful restart recovery, both in cases of a routing protocol process (rpd) restart and graceful Routing Engine switchover.</p> <p>Bidirectional PIM accepts packets for a bidirectional route on multiple interfaces. This means that some topologies might develop multicast routing loops if all PIM neighbors are not synchronized with regard to the identity of the designated forwarder (DF) on each link. If one routing device is forwarding without actively participating in DF elections, particularly after unicast routing changes, multicast routing loops might occur.</p> <p>If graceful restart for PIM is enabled and the forwarding of packets on bidirectional routes is disallowed (by including the no-bidirectional-mode statement in the configuration), PIM behaves conservatively to avoid multicast routing loops during the recovery period. When the routing protocol process (rpd) restarts, all bidirectional routes are deleted. After graceful restart has completed, the routes are re-added, based on the converged unicast and bidirectional PIM state. While graceful restart is active, bidirectional multicast flows drop packets.</p>
Default	If graceful restart for PIM is enabled and the bidirectional PIM is enabled, the default graceful restart behavior is to continue forwarding packets on bidirectional routes. If the gracefully restarting routing device was serving as a DF for some interfaces to rendezvous points, the restarting routing device sends a DF Winner message with a metric of 0 on each of these RP interfaces. This ensures that a neighbor routing device does not become the DF due to unicast topology changes that might occur during the graceful restart period. Sending a DF Winner message with a metric of 0 prevents another PIM neighbor from assuming the DF role until after graceful restart completes. When graceful restart completes, the gracefully restarted routing device sends another DF Winner message with the actual converged unicast metric.



NOTE: Graceful Routing Engine switchover operates independently of the graceful restart behavior. If graceful Routing Engine switchover is configured without graceful restart, all PIM routes for all modes are deleted when the rpd process restarts. If graceful Routing Engine switchover is configured with graceful restart, the behavior is the same as described here, except that the recovery happens on the Routing Engine that assumes mastership.

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> in the <i>Multicast Protocols Feature Guide for Routing Devices</i>• <i>Understanding Bidirectional PIM</i>• <i>Example: Configuring Bidirectional PIM</i>

no-dr-flood (PIM Snooping)

Syntax	no-dr-flood;
Hierarchy Level	[edit routing-instances <instance-name> protocols pim-snooping traceoptions], [edit logical-systems <logical-system-name> routing-instances <instance-name> protocols pim-snooping traceoptions], [edit routing-instances <instance-name> protocols pim-snooping vlan <vlan-id>], [edit logical-systems <logical-system-name> routing-instances <instance-name> protocols pim-snooping vlan <vlan-id>]
Release Information	Statement introduced in Junos OS Release 12.3 for MX Series 3D Universal Edge Routers. Statement introduced in Junos OS Release 13.2 for M Series Multiservice Edge Routers.
Description	Disable default flooding of multicast data on the PIM designated router port.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

offer-period

Syntax	<code>offer-period milliseconds;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim interface interface-name bidirectional df-election],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim interface interface-name bidirectional df-election],</p> <p>[edit protocols pim interface interface-name bidirectional df-election],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim interface interface-name bidirectional df-election]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 13.3 for the PTX5000 router.</p>
Description	<p>Configure the designated forwarder (DF) election offer period for bidirectional PIM. When a DF election Offer or Winner message fails to be received, the message is retransmitted. The offer-period statement modifies the interval between repeated DF election messages. The robustness-count statement determines the minimum number of DF election messages that must fail to be received for DF election to fail. To prevent routing loops, all routing devices on the link must have a consistent view of the DF. When the DF election fails because DF election messages are not received, forwarding on bidirectional PIM routes is suspended.</p> <p>If a router receives from a neighbor a better offer than its own, the router stops participating in the election for a period of robustness-count * offer-period. Eventually, all routers except the best candidate stop sending Offer messages.</p>
Options	<p>milliseconds—Interval to wait before retransmitting DF Offer and Winner messages.</p> <p>Range: 100 through 10,000 milliseconds</p> <p>Default: 100</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>Understanding Bidirectional PIM</i> • <i>Example: Configuring Bidirectional PIM</i> • robustness-count on page 373

override (PIM static RP)

Syntax	override;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp local],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp local family inet],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp local family inet6],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp static address <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols pim rp local],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols pim rp local family inet],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols pim rp local family inet6],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols pim rp static address <i>address</i>],</p> <p>[edit protocols pim rp local],</p> <p>[edit protocols pim rp local family inet],</p> <p>[edit protocols pim rp local family inet6],</p> <p>[edit protocols pim rp static address <i>address</i>],</p> <p>[edit routing-instances <i>instance-name</i> protocols pim rp local],</p> <p>[edit routing-instances <i>instance-name</i> protocols pim rp local family inet],</p> <p>[edit routing-instances <i>instance-name</i> protocols pim rp local family inet6],</p> <p>[edit routing-instances <i>instance-name</i> protocols pim rp static address <i>address</i>]</p>
Release Information	Statement introduced in Junos OS Release 11.4.
Description	When you configure both static RP mapping and dynamic RP mapping (such as auto-RP) in a single routing instance, allow the static mapping to take precedence for a given group range, and allow dynamic RP mapping for all other groups.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Static RP on page 106 • Configuring PIM Auto-RP on page 99

override-interval

Syntax	<code>override-interval <i>milliseconds</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim],</p> <p>[edit logical-systems <i>logical-system-name</i> 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 interface <i>interface-name</i>],</p> <p>[edit protocols pim],</p> <p>[edit protocols pim interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim]</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.1.</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	Set the maximum time in milliseconds to delay sending override join messages for a multicast network that has join suppression enabled. When a router or switch sees a prune message for a join it is currently suppressing, it waits for the interval specified by the override timer before it sends an override join message.
Options	<p>This is a random timer with a value in milliseconds.</p> <p>Range: 0 through maximum override value</p> <p>Default: 2000 milliseconds</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: Enabling Join Suppression • propagation-delay on page 368 • reset-tracking-bit on page 370

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>• Configuring PIM Dense Mode Properties on page 95• Configuring PIM Sparse-Dense Mode Properties on page 97

pim-snooping

Syntax	<pre> pim-snooping { no-dr-flood; traceoptions{ file [filename files no-word-readable size word-readable]; flag [all general hello join normal packets policy prune route state task timer]; } vlan<vlan-id>{ no-dr-flood; } } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> instance-type <i>vpls</i> protocols],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols],</p> <p>[edit routing-instances <i>instance-name</i> protocols]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.3 for MX Series 3D Universal Edge Routers.</p> <p>Statement introduced in Junos OS Release 13.2 for M Series Multiservice Edge Routers.</p>
Description	<p>PIM snooping snoops PIM hello and join/prune packets on each interface to find interested multicast receivers and then populates the multicast forwarding tree with the information. PIM snooping is configured on PE routers connected using pseudowires and ensures that no new PIM packets are generated in the VPLS (with the exception of PIM messages sent through LDP on pseudowires). PIM snooping differs from PIM proxying in that PIM snooping floods both the PIM hello and join/prune packets in the VPLS, whereas PIM proxying only floods hello packets.</p>
Default	PIM snooping is disabled on the device.
Options	<p>no-dr-flood—Disable default flooding of multicast data on the PIM-designated router port.</p> <p>traceoptions—Configure tracing options for PIM snooping.</p> <p>vlan <vlan-id>—Configure PIM snooping parameters for a VLAN.</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"> • PIM Snooping for VPLS on page 159

prefix-list (PIM RPF Selection)

Syntax	<pre>prefix-list <i>prefix-list-addresses</i> { source <i>source-address</i> { next-hop <i>next-hop-address</i>; } wildcard-source { next-hop <i>next-hop-address</i>; } }</pre>
Hierarchy Level	<pre>[edit routing-instances <i>routing-instance-name</i> protocols pim rpf-selection group <i>group-address</i> source <i>source-address</i>], [edit routing-instances <i>routing-instance-name</i> protocols pim rpf-selection group <i>group-address</i> wildcard-source], [edit routing-instances <i>routing-instance-name</i> protocols pim rpf-selection prefix-list <i>prefix-list-addresses</i> source <i>source-address</i>], [edit routing-instances <i>routing-instance-name</i> protocols pim rpf-selection prefix-list <i>prefix-list-addresses</i> wildcard-source]</pre>
Release Information	Statement introduced in Junos OS Release 10.4. 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	(Optional) Configure a list of prefixes (addresses) for multiple PIM groups.
Options	<p><i>prefix-list-addresses</i>—List of prefixes (addresses) for multiple PIM groups.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	view-level—To view this statement in the configuration. control-level—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring PIM RPF Selection</i>

priority (Bootstrap)

Syntax	<code>priority <i>number</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols <code>pim rp bootstrap</code> (inet inet6)],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols <code>pim rp bootstrap</code> (inet inet6)],</p> <p>[edit protocols <code>pim rp bootstrap</code> (inet inet6)],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols <code>pim rp bootstrap</code> (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"> • Configuring PIM Bootstrap Properties for IPv4 on page 113 • Configuring PIM Bootstrap Properties for IPv4 or IPv6 on page 114 • bootstrap-priority on page 311

priority (PIM Interfaces)

Syntax	<code>priority <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols <code>pim interface <i>interface-name</i></code>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols <code>pim interface <i>interface-name</i></code>], [edit protocols <code>pim interface <i>interface-name</i></code>], [edit routing-instances <i>routing-instance-name</i> protocols <code>pim interface <i>interface-name</i></code>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. 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	<i>number</i> —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">• Configuring Interface Priority for PIM Designated Router Selection on page 90

priority (PIM RPs)

Syntax	<code>priority <i>number</i>;</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>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	<p>For PIM-SM, configure this routing device's priority for becoming an RP.</p> <p>For bidirectional PIM, configure this RP address' priority for becoming an RP.</p> <p>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.</p>
Options	<p><i>number</i>—Priority for becoming an RP. A lower value corresponds to a higher priority.</p> <p>Range: 0 through 255</p> <p>Default: 1</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Local PIM RPs on page 107 in the <i>Multicast Protocols Feature Guide for Routing Devices</i> • <i>Example: Configuring Bidirectional PIM</i>

propagation-delay

Syntax	<code>propagation-delay <i>milliseconds</i>;</code>
Hierarchy Level	<code>[edit protocols pim],</code> <code>[edit protocols pim interface <i>interface-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols pim],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> protocols pim],</code> <code>[edit logical-systems <i>logical-system-name</i> protocols pim interface <i>interface-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols</code> <code>pim interface <i>interface-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 10.1. 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	Set a delay for implementing a PIM prune message on the upstream routing device on a multicast network for which join suppression has been enabled. The routing device waits for the prune pending period to detect whether a join message is currently being suppressed by another routing device.
Options	<i>milliseconds</i> —Interval for the prune pending timer, which is the sum of the propagation-delay value and the override-interval value. Range: 250 through 2000 milliseconds Default: 500 milliseconds
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: Enabling Join Suppression</i>• override-interval on page 357• reset-tracking-bit on page 370

register-limit

Syntax	<pre> register-limit { family (inet inet6) { log-interval <i>seconds</i>; maximum <i>limit</i>; threshold <i>value</i>; } log-interval <i>seconds</i>; maximum <i>limit</i>; threshold <i>value</i>; } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp],</p> <p>[edit protocols pim rp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp]</p>
Release Information	Statement introduced in Junos OS Release 12.2.
Description	Configure a limit for the number of incoming (S,G) PIM registers.



NOTE: The maximum limit settings that you configure with the `maximum` and the `family (inet | inet6) maximum` statements are mutually exclusive. For example, if you configure a global maximum PIM register message limit, you cannot configure a limit at the family level for IPv4 or IPv6. If you attempt to configure a limit at both the global level and the family level, the device will not accept the configuration.

Options	<p>family (inet inet6)—(Optional) Specify either IPv4 or IPv6 messages to be counted towards the configured register message limit.</p> <p>Default: Both IPv4 and IPv6 messages are counted towards the configured register message limit.</p> <p>The remaining statements are described 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 PIM State Limits • clear pim join on page 506 • clear pim register on page 510

reset-tracking-bit

Syntax	reset-tracking-bit;
Hierarchy Level	[edit protocols pim], [edit protocols pim interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> protocols pim], [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>]
Release Information	Statement introduced in Junos OS Release 10.1. 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	Change the value of a tracking bit (T-bit) field in the LAN prune delay hello option from the default of 1 to 0, which enables join suppression for a multicast interface. When the network starts receiving multiple identical join messages, join suppression triggers a random timer with a value of 66 through 84 milliseconds ($1.1 \times \text{periodic}$ through $1.4 \times \text{periodic}$, where periodic is 60 seconds). This creates an interval during which no identical join messages are sent. Eventually, only one of the identical messages is sent. Join suppression is triggered each time identical messages are sent for the same join.
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: Enabling Join Suppression</i>• override-interval on page 357• propagation-delay on page 368

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>

robustness-count

Syntax	<code>robustness-count <i>number</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim interface <i>interface-name</i> bidirectional df-election],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> bidirectional df-election],</p> <p>[edit protocols pim interface <i>interface-name</i> bidirectional df-election],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> bidirectional df-election]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 13.3 for the PTX5000 router.</p>
Description	<p>Configure the designated forwarder (DF) election robustness count for bidirectional PIM. When a DF election Offer or Winner message fails to be received, the message is retransmitted. The robustness-count statement sets the minimum number of DF election messages that must fail to be received for DF election to fail. To prevent routing loops, all routers on the link must have a consistent view of the DF. When the DF election fails because DF election messages are not received, forwarding on bidirectional PIM routes is suspended.</p> <p>If a router receives from a neighbor a better offer than its own, the router stops participating in the election for a period of robustness-count * offer-period. Eventually, all routers except the best candidate stop sending Offer messages.</p>
Options	<p><i>number</i>—Number of transmission attempts for DF election messages.</p> <p>Range: 1 through 10</p> <p>Default: 3</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>Understanding Bidirectional PIM</i> • <i>Example: Configuring Bidirectional PIM</i>

rp

```

Syntax  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-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 on page 128](#)
- [dr-register-policy on page 317](#)


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>

rpf-selection

Syntax	<pre> 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; } } } </pre>
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> protocols pim]
Release Information	<p>Statement introduced in JUNOS Release 10.4.</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 the PIM RPF next-hop neighbor for a specific group and source for a VRF routing instance.</p> <p>The remaining statements are explained separately.</p>
Default	If you omit the rpf-selection statement, PIM RPF checks typically choose the best path determined by the unicast protocol for all multicast flows.
Options	source-address —Specific source address for the PIM group.
Required Privilege Level	<p>view-level—To view this statement in the configuration.</p> <p>control-level—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring PIM RPF Selection</i>

sglimit

Syntax	<pre>sglimit { family (inet inet6) { log-interval seconds; maximum limit; threshold value; } log-interval seconds; maximum limit; threshold value; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim]</p>
Release Information	Statement introduced in Junos OS Release 12.2.
Description	Configure a limit for the number of accepted (*G) and (S,G) PIM join states.
<div>  <p>NOTE: The maximum limit settings that you configure with the <code>maximum</code> and the <code>family (inet inet6) maximum</code> statements are mutually exclusive. For example, if you configure a global maximum PIM join state limit, you cannot configure a limit at the family level for IPv4 or IPv6 joins. If you attempt to configure a limit at both the global level and the family level, the device will not accept the configuration.</p> </div>	
Options	<p>family (inet inet6)—(Optional) Specify either IPv4 or IPv6 join states to be counted towards the configured join state limit.</p> <p>Default: Both IPv4 and IPv6 join states are counted towards the configured join state limit.</p> <p>The remaining statements are described 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 PIM State Limits • clear pim join on page 506

source (PIM RPF Selection)

Syntax	<code>source source-address { next-hop next-hop-address; }</code>
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> protocols pim rpf-selection group <i>group-address</i>], [edit routing-instances <i>routing-instance-name</i> protocols pim rpf-selection prefix-list <i>prefix-list-addresses</i>]
Release Information	Statement introduced in JUNOS Release 10.4. 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 source address for the PIM group.
Options	source-address —Specific source address for the PIM group. The remaining statements are explained separately.
Required Privilege Level	view-level—To view this statement in the configuration. control-level—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring PIM RPF Selection</i>

spt-threshold

Syntax	spt-threshold { infinity [<i>policy-names</i>]; }
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	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. 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>Example: Configuring the PIM SPT Threshold Policy</i>


standby-path-creation-delay

Syntax	<code>standby-path-creation-delay <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 in Junos OS Release 12.2.
Description	<p>Configure the time interval after which a standby path is created, when a new ECMP interface or neighbor is added to the network.</p> <p>In the absence of this statement, ECMP joins are redistributed as soon as a new ECMP interface or neighbor is added to the network.</p>
Options	<code><seconds></code> —Time interval after which a standby path is created, when a new ECMP interface or neighbor is added to the network. Range is from 1 through 300.
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 PIM Make-Before-Break Join Load Balancing</i>• <i>Configuring PIM Join Load Balancing</i>• clear pim join-distribution on page 508• join-load-balance on page 337• idle-standby-path-switchover-delay on page 331


static (Protocols PIM)

Syntax	<pre>static { address address { group-ranges { destination-ip-prefix</prefix-length>; } override; version version; } }</pre>
Hierarchy Level	<p>[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]</p>
Release Information	<p>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.</p>
Description	<p>Configure static RP addresses. The default static RP address is 224.0.0.0/4. To configure other addresses, include one or more address statements. You can configure a static RP in a logical system only if the logical system is not directly connected to a source.</p> <p>For each static RP address, you can optionally specify the PIM version and the groups for which this address can be the RP. The default PIM version is version 1.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Static PIM RP Address on the Non-RP Routing Device on page 111

threshold (PIM BFD Detection Time)

Syntax	<code>threshold <i>milliseconds</i>;</code>
Hierarchy Level	[edit protocols pim interface <i>interface-name</i> bfd-liveness-detection detection-time], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> bfd-liveness-detection detection-time]
Release Information	Statement introduced in Junos OS Release 8.2. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for BFD authentication introduced in Junos OS Release 9.6. 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 threshold for the adaptation of the BFD session detection time. When the detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.
<div>  <p>NOTE: The threshold value must be equal to or greater than the transmit interval.</p> <p>The threshold time must be equal to or greater than the value specified in the minimum-interval or the minimum-receive-interval statement.</p> </div>	
Options	<i>milliseconds</i> —Value for the detection time adaptation threshold. Range: 1 through 255,000
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 BFD for PIM on page 133 • bfd-liveness-detection on page 305 • detection-time on page 313 • minimum-interval on page 347 • minimum-receive-interval on page 349

threshold (PIM BFD Transmit Interval)

Syntax	<code>threshold <i>milliseconds</i>;</code>
Hierarchy Level	[edit protocols pim interface <i>interface-name</i> bfd-liveness-detection transmit-interval], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> bfd-liveness-detection transmit-interval]
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 12.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the threshold for the adaptation of the BFD session transmit interval. When the transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent.
Options	<i>milliseconds</i> —Value for the transmit interval adaptation threshold. Range: 0 through 4,294,967,295 ($2^{32} - 1$)
<div>  <p>NOTE: The threshold value specified in the <code>threshold</code> statement must be greater than the value specified in the <code>minimum-interval</code> statement for the <code>transmit-interval</code> statement.</p> </div>	
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring BFD for PIM on page 133 • bfd-liveness-detection on page 305

threshold (PIM Entries)

Syntax	<code>threshold <i>value</i>;</code>
Hierarchy Level	<pre> [edit logical-systems <i>logical-system-name</i> protocols pim sglimit], [edit logical-systems <i>logical-system-name</i> protocols pim sglimit <i>family</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim sglimit], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim sglimit <i>family</i>], [edit protocols pim sglimit], [edit protocols pim sglimit <i>family</i>], [edit routing-instances <i>routing-instance-name</i> protocols pim sglimit], [edit routing-instances <i>routing-instance-name</i> protocols pim sglimit <i>family</i>], [edit logical-systems <i>logical-system-name</i> protocols pim rp group-rp-mapping], [edit logical-systems <i>logical-system-name</i> protocols pim rp group-rp-mapping <i>family</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp group-rp-mapping], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp group-rp-mapping <i>family</i>], [edit protocols pim rp group-rp-mapping], [edit protocols pim rp group-rp-mapping <i>family</i>], [edit routing-instances <i>routing-instance-name</i> protocols pim rp group-rp-mapping], [edit routing-instances <i>routing-instance-name</i> protocols pim rp group-rp-mapping <i>family</i>], [edit logical-systems <i>logical-system-name</i> protocols pim rp register-limit], [edit logical-systems <i>logical-system-name</i> protocols pim rp register-limit <i>family</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp register-limit], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp register-limit <i>family</i>], [edit protocols pim rp register-limit], [edit protocols pim rp register-limit <i>family</i>], [edit routing-instances <i>routing-instance-name</i> protocols pim rp register-limit], [edit routing-instances <i>routing-instance-name</i> protocols pim rp register-limit <i>family</i>], </pre>
Release Information	Statement introduced in Junos OS Release 12.2.
Description	Configure a threshold at which a warning message is logged when a certain number of PIM entries have been received by the device.
Options	<p><i>value</i>—Threshold at which a warning message is logged. This is a percentage of the maximum number of entries accepted by the device as defined with the maximum statement. You can apply this threshold to incoming PIM join messages, PIM register messages, and group-to-RP mappings.</p> <p>For example, if you configure a maximum number of 1,000 incoming group-to-RP mappings, and you configure a threshold value of 90 percent, warning messages are logged in the system log when the device receives 900 group-to-RP mappings. The same formula applies to incoming PIM join messages and PIM register messages if configured with both the maximum limit and the threshold value statements.</p> <p>Default: 1 through 100</p>

Required Privilege	routing—To view this statement in the configuration.
Level	routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• add new concept and example topic to related topic list.• clear pim join on page 506

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	<p>[edit logical-systems <i>logical-system-name</i> protocols pim],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim],</p> <p>[edit protocols pim],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <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 PIM tracing options.</p> <p>To specify more than one tracing operation, include multiple flag statements.</p>
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</p> <p>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	• Configuring PIM Trace Options on page 82
	• Tracing DVMRP Protocol Traffic
	• Tracing MSDP Protocol Traffic
	• Configuring PIM Trace Options on page 82

traceoptions (PIM Snooping)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i> <<i>flag-modifier</i>> <disable>; } </pre>
Hierarchy Level	[edit routing-instances < <i>instance-name</i> > protocols pim-snooping], [edit logical-systems < <i>logical-system-name</i> > routing-instances < <i>instance-name</i> > protocols pim-snooping]
Release Information	Statement introduced in Junos OS Release 12.3 for MX Series 3D Universal Edge devices. Statement introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.
Description	Define tracing operations for PIM snooping.
Default	<p>The traceoptions feature is disabled by default.</p> <p>The default PIM trace options are those inherited from the routing protocol's traceoptions statement included at the [edit routing-options] hierarchy level.</p>
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>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.</p> <p>PIM Snooping Tracing Flags:</p> <ul style="list-style-type: none"> • all—All tracing operations. • general—Trace general PIM snooping events. • hello—Trace hello packets. • join—Trace join messages. • normal—Trace normal PIM snooping events. If you do not specify this flag, only unusual or abnormal operations are traced. • packets—Trace all PIM packets. • policy—Trace policy processing. • prune—Trace prune messages. • route—Trace routing information. • state—Trace PIM state transitions. • task—Trace PIM protocol task processing. • timer—Trace PIM protocol timer processing. <p><i>flag-modifier</i>—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers per flag:</p>

- **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.

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

Related Documentation

- [PIM Snooping for VPLS on page 159](#)

transmit-interval (PIM BFD Liveness Detection)

Syntax `transmit-interval {
 minimum-interval milliseconds;
 threshold milliseconds;
}`

Hierarchy Level [edit protocols pim interface *interface-name* bfd-liveness-detection],
[edit routing-instances *routing-instance-name* protocols pim interface *interface-name* bfd-liveness-detection]

Release Information Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for BFD authentication introduced in Junos OS Release 9.6.
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 transmit interval for the **bfd-liveness-detection** statement. The negotiated transmit interval for a peer is the interval between the sending of BFD packets to peers. The receive interval for a peer is the minimum interval between receiving packets sent from its peer; the receive interval is not negotiated between peers. To determine the transmit interval, each peer compares its configured minimum transmit interval with its peer's minimum receive interval. The larger of the two numbers is accepted as the transmit interval for that peer.

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

- [Configuring BFD for PIM on page 133](#)
- [bfd-liveness-detection on page 305](#)
- [threshold on page 385](#)
- [minimum-interval on page 348](#)
- [minimum-receive-interval on page 349](#)

tunnel-devices (Tunnel-Capable PICs)

Syntax	<code>tunnel-devices [<i>mt-fpc/pic/port</i>];</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>instance-name</i> protocols pim], [edit routing-instances <i>instance-name</i> protocols pim]
Release Information	Statement introduced in Junos OS Release 10.2. Statement introduced in Junos OS Release 10.2 for EX Series switches.
Description	<p>List one or more tunnel-capable PICs to be used for creating multicast tunnel (mt) interfaces. Creating a PIC list enables you to control the load-balancing implementation.</p> <p>Tunnel-capable PICs include:</p> <ul style="list-style-type: none"> • Adaptive Services PIC • Multiservices PIC or Multiservices DPC • Tunnel Services PIC • On MX Series routers, a PIC created with the tunnel-services statement at the [edit chassis fpc <i>slot-number</i> pic <i>number</i>] hierarchy level. <p>The physical position of the PIC in the routing device determines the multicast tunnel interface name. For example, if you have an Adaptive Services PIC installed in FPC slot 0 and PIC slot 0, the corresponding multicast tunnel interface name is mt-0/0/0. The same is true for Tunnel Services PICs, Multiservices PICs, and Multiservices DPCs.</p>
Default	Multicast tunnel interfaces are created on all available tunnel-capable PICs, based on a round-robin algorithm.
Options	mt-fpc/pic/port —Interface that is automatically generated when a tunnel-capable PIC is installed in 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>Load Balancing Multicast Tunnel Interfaces Among Available PICs</i>

version (BFD)

Syntax	version (0 1 automatic);
Hierarchy Level	[edit protocols piminterface <i>interface-name</i> bfd-liveness-detection], [edit routing-instances <i>routing-instance-name</i> protocols pim interface <i>interface-name</i> bfd-liveness-detection]
Release Information	Statement introduced in Junos OS Release 8.1. 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 bidirectional forwarding detection (BFD) protocol version that you want to detect.
Options	Configure the BFD version to detect: 1 (BFD version 1) or automatic (autodetect the BFD version) Default: automatic
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 BFD for PIM on page 133

version (PIM)

Syntax	<code>version version;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim interface interface-name],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols pim rp static address address],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim interface interface-name],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp static address address],</p> <p>[edit protocols pim interface interface-name],</p> <p>[edit protocols pim rp static address address],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim interface interface-name],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp static address address]</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>
Description	Specify the version of PIM.
Options	<p>version—PIM version number.</p> <p>Range: 1 or 2</p> <p>Default: PIMv1 for rendezvous point (RP) mode (at the [edit protocols pim rp static address address] hierarchy level). PIMv2 for interface mode (at the [edit protocols pim interface interface-name] hierarchy level).</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Enabling PIM Sparse Mode • Configuring PIM Dense Mode Properties on page 95 • Configuring PIM Sparse-Dense Mode Properties on page 97

vlan (PIM Snooping)

Syntax	<code>vlan <vlan-id>{ no-dr-flood; }</code>
Hierarchy Level	[edit routing-instances <instance-name> protocols pim-snooping], [edit logical-systems <logical-system-name> routing-instances <instance-name> protocols pim-snooping]
Release Information	Statement introduced in Junos OS Release 12.3 for MX Series 3D Universal Edge devices. Statement introduced in Junos OS Release 13.2 for M Series Multiservice Edge devices.
Description	Configure PIM snooping parameters for a 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">• PIM Overview on page 73• Configuring Basic PIM Settings on page 77

vpn-group-address

Syntax	<code>vpn-group-address address;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim], [edit routing-instances <i>routing-instance-name</i> protocols pim]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the group address for the Layer 3 VPN in the service provider's network.
Options	<i>address</i> —Address for the Layer 3 VPN in the service provider's network.
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 Multicast Layer 3 VPNs• Multicast Protocols Feature Guide for Routing Devices

wildcard-source (PIM RPF Selection)

Syntax	wildcard-source { next-hop next-hop-address; }
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> protocols pim rpf-selection group <i>group-address</i>], [edit routing-instances <i>routing-instance-name</i> protocols pim rpf-selection prefix-list <i>prefix-list-addresses</i>]
Release Information	Statement introduced in Junos OS Release 10.4. 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	Use a wildcard for the multicast source instead of (or in addition to) a specific multicast source. The remaining statements are explained separately.
Required Privilege Level	view-level—To view this statement in the configuration. control-level—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring PIM RPF Selection</i>

CHAPTER 18

Operational Commands: IGMP

- `clear igmp statistics`
- `show igmp group`
- `show igmp interface`
- `show multicast pim-to-igmp-proxy`

clear igmp statistics

List of Syntax	Syntax on page 400 Syntax (EX Series Switches) on page 400
Syntax	clear igmp statistics <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Syntax (EX Series Switches)	clear igmp statistics <interface <i>interface-name</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.3 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX 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
Related Documentation	<ul style="list-style-type: none"> show igmp statistics
List of Sample Output	clear igmp statistics on page 400
Output Fields	See <i>show igmp statistics</i> 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
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		

show igmp group

List of Syntax	Syntax on page 402 Syntax (EX Series Switch and the QFX Series) on page 402
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> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX 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
Related Documentation	<ul style="list-style-type: none"> clear igmp membership
List of Sample Output	show igmp group (Include Mode) on page 403 show igmp group (Exclude Mode) on page 404 show igmp group brief on page 404 show igmp group detail on page 404
Output Fields	Table 8 on page 402 describes the output fields for the show igmp group command. Output fields are listed in the approximate order in which they appear.

Table 8: 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

Table 8: show igmp group Output Fields (*continued*)

Field Name	Field Description	Level of Output
Group Mode	Mode the SSM group is operating in: Include or Exclude .	All levels
Source	Source address.	All levels
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 406 Syntax (EX Series Switches and the QFX Series) on page 406
Syntax	<pre>show igmp interface <brief detail> <interface-name> <logical-system (all logical-system-name)></pre>
Syntax (EX Series Switches 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> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX 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
List of Sample Output	show igmp interface on page 408 show igmp interface brief on page 409 show igmp interface detail on page 409 show igmp interface <interface-name> on page 409
Output Fields	<p>Table 9 on page 406 describes the output fields for the show igmp interface command. Output fields are listed in the approximate order in which they appear.</p>

Table 9: show igmp interface Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface.	All levels

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

Field Name	Field Description	Level of Output
Querier	Address of the routing device that has been elected to send membership queries.	All levels
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
Group limit	Maximum number of groups allowed on the interface. Any joins requested after the limit is reached are rejected.	All levels
Group threshold	Configured threshold at which a warning message is generated. This threshold is based on a percentage of groups received on the interface. If the number of groups received reaches the configured threshold, the device generates a warning message.	All levels
Group log-interval	Time (in seconds) between consecutive log messages.	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

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

Field Name	Field Description	Level of Output
Passive	<p>State of the passive mode option:</p> <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
Configured Parameters	<p>Information configured by the user:</p> <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	<p>Derived information:</p> <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 408](#).

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 408](#).

show igmp interface <interface-name>

```

user@host# show igmp interface ge-3/2/0.0
Interface: ge-3/2/0.0
Querier: 20.1.1.1
State: Up Timeout:    None Version:  3 Groups:      1
Group limit: 8
Group threshold: 60
Group log-interval: 10
Immediate leave: Off
Promiscuous mode: Off

```

show multicast pim-to-igmp-proxy

List of Syntax	Syntax on page 410 Syntax (EX Series Switch and the QFX Series) on page 410
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 10.3.</p> <p>instance option introduced in Junos OS Release 10.3 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	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
Related Documentation	<ul style="list-style-type: none"> Configuring PIM-to-IGMP and PIM-to-MLD Message Translation
List of Sample Output	show multicast pim-to-igmp-proxy on page 411 show multicast pim-to-igmp-proxy instance on page 411
Output Fields	<p>Table 10 on page 410 describes the output fields for the show multicast pim-to-igmp-proxy command. Output fields are listed in the order in which they appear.</p>

Table 10: show multicast pim-to-igmp-proxy Output Fields

Field Name	Field Description
Instance	Routing instance. Default instance is master (inet.0 routing table).

Table 10: show multicast pim-to-igmp-proxy Output Fields (*continued*)

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

Sample Output

show multicast pim-to-igmp-proxy

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

show multicast 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
```


CHAPTER 19

Operational Commands: IGMP Snooping

- clear igmp snooping membership
- clear igmp snooping statistics
- show igmp snooping interface
- show igmp snooping membership
- show igmp snooping statistics

clear igmp snooping membership

Syntax	<code>clear igmp snooping membership</code> <code><group source address></code> <code><instance <i>instance-name</i>></code> <code><interface <i>interface-name</i>></code> <code><learning-domain <i>learning-domain-name</i>></code> <code><logical-system <i>logical-system-name</i>></code> <code><vlan-id <i>vlan-identifier</i>></code>
Release Information	Command introduced in Junos OS Release 8.5.
Description	Clear IP IGMP snooping membership information.
Options	<p>none—Clear IGMP snooping membership for all supported address families on all interfaces.</p> <p>group source address—(Optional) Clear IGMP snooping membership for the specified multicast group or source address.</p> <p>instance <i>instance-name</i>—(Optional) Clear IGMP snooping membership for the specified instance.</p> <p>interface <i>interface-name</i>—(Optional) Clear IGMP snooping membership on a specific interface.</p> <p>learning-domain <i>learning-domain-name</i>—(Optional) Perform this operation on all learning domains or on a particular learning domain.</p> <p>logical-system <i>logical-system-name</i>—(Optional) Display information about a particular logical system, or for all logical systems.</p> <p>vlan-id <i>vlan-identifier</i>—(Optional) Perform this operation on a particular VLAN.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show igmp snooping membership on page 421
List of Sample Output	clear igmp snooping membership on page 414
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear igmp snooping membership

```
user@host> clear igmp snooping membership
```


clear igmp snooping statistics

Syntax	clear igmp snooping statistics <instance <i>instance-name</i> > <interface <i>interface-name</i> > <learning-domain (all <i>learning-domain-name</i>)> <logical-system <i>logical-system-name</i> >
Release Information	Command introduced in Junos OS Release 8.5.
Description	Clear IP IGMP snooping statistics.
Options	<p>none—Clear IGMP snooping statistics for all supported address families on all interfaces.</p> <p>instance <i>instance-name</i>—(Optional) Clear IGMP snooping statistics for the specified instance.</p> <p>interface <i>interface-name</i>—(Optional) Clear IGMP snooping statistics on a specific interface.</p> <p>learning-domain (all <i>learning-domain-name</i>)—(Optional) Perform this operation on all learning domains or on a particular learning domain.</p> <p>logical-system <i>logical-system-name</i>—(Optional) Delete the IGMP snooping statistics for a given logical system or for all logical systems.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show igmp snooping statistics on page 425
List of Sample Output	clear igmp snooping statistics on page 415
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear igmp snooping statistics

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

show igmp snooping interface

Syntax	show igmp snooping interface <i>interface-name</i> <brief detail> <bridge-domain <i>bridge-domain-name</i> > <logical-system <i>logical-system-name</i> > <virtual-switch <i>virtual-switch-name</i> > <vlan-id <i>vlan-identifier</i> >
Release Information	Command introduced in Junos OS Release 8.5.
Description	Display IGMP snooping interface information.
Options	<p>none —Display detailed information.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>bridge-domain <i>bridge-domain-name</i>—(Optional) Display information about a particular bridge domain.</p> <p>logical-system <i>logical-system-name</i>—(Optional) Display information about a particular logical system, or type 'all'.</p> <p>virtual-switch <i>virtual-switch-name</i>—(Optional) Display information about a particular virtual switch.</p> <p>vlan-id <i>vlan-identifier</i>—(Optional) Display information about a particular VLAN.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show igmp snooping membership on page 421 • show igmp snooping statistics on page 425
List of Sample Output	show igmp snooping interface on page 417 show igmp snooping interface (Group Limit Configured) on page 419
Output Fields	Table 11 on page 416 lists the output fields for the show igmp snooping interface command. Output fields are listed in the approximate order in which they appear.

Table 11: show igmp snooping interface Output Fields

Field Name	Field Description	Level of Output
Routing-instance	Routing instance for IGMP snooping.	All levels
Learning Domain	Learning domain for snooping.	All levels
IGMP Query Interval	Frequency (in seconds) with which this router sends membership queries when it is the querier.	detail

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

Field Name	Field Description	Level of Output
IGMP Query Response Interval	Time (in seconds) that the router waits for a response to a general query.	detail
IGMP Last Member Query Interval	Time (in seconds) that the router waits for a report in response to a group-specific query.	detail
IGMP Robustness Count	Number of times the router retries a query.	detail
immediate-leave	State of immediate leave: On or Off .	All levels
router-interface	Router interfaces that are part of this learning domain.	All levels
Group limit	Maximum number of (source,group) pairs allowed per interface. When a group limit is not configured, this field is not shown.	All levels
interface	Interfaces that are being snooped in this learning domain.	All levels
Groups	Number of groups on the interface.	none
State	State of the interface: Up or Down .	none
Up Groups	Number of active multicast groups attached to the logical interface.	All levels
IGMP Membeship Timeout	Timeout for group membership. If no report is received for these groups before the timeout expires, the group membership is removed.	none
IGMP Other Querier Present Timeout	Time that the router waits for the IGMP querier to send a query.	none

Sample Output

show igmp snooping interface

```

user@host> show igmp snooping interface logical-system all
logical-system: default
Instance: VPLS-6
Learning-Domain: default
Interface: ge-0/2/2.601
    State:          Up Groups:      10
    Immediate leave: Off
    Router interface: no

Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2

Instance: VS-4
Bridge-Domain: VS-4-BD-1

```

```
Learning-Domain: vlan-id 1041
Interface: ae2.3
    State:          Up Groups:      0
    Immediate leave: Off
    Router interface: no
Interface: ge-0/2/2.1041
    State:          Up Groups:      20
    Immediate leave: Off
    Router interface: no
```

```
Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2
```

```
Instance: default-switch
Bridge-Domain: bd-200
Learning-Domain: default
Interface: ge-0/2/2.100
    State:          Up Groups:      20
    Immediate leave: Off
    Router interface: no
```

```
Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2
```

```
Bridge-Domain: bd0
Learning-Domain: default
Interface: ae0.0
    State:          Up Groups:      0
    Immediate leave: Off
    Router interface: yes
Interface: ae1.0
    State:          Up Groups:      0
    Immediate leave: Off
    Router interface: no
Interface: ge-0/2/2.0
    State:          Up Groups:      32
    Immediate leave: Off
    Router interface: no
```

```
Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2
```

```
Instance: VPLS-1
Learning-Domain: default
Interface: ge-0/2/2.502
    State:          Up Groups:      11
    Immediate leave: Off
    Router interface: no
```

```
Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
```

```
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2
```

```
Instance: VS-1
Bridge-Domain: VS-BD-1
Learning-Domain: default
Interface: ae2.0
    State:          Up Groups:      0
    Immediate leave: Off
    Router interface: no
Interface: ge-0/2/2.1010
    State:          Up Groups:      20
    Immediate leave: Off
    Router interface: no
```

```
Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2
```

```
Bridge-Domain: VS-BD-2
Learning-Domain: default
Interface: ae2.0
    State:          Up Groups:      0
    Immediate leave: Off
    Router interface: no
Interface: ge-0/2/2.1011
    State:          Up Groups:      20
    Immediate leave: Off
    Router interface: no
```

```
Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2
```

```
Instance: VPLS-p2mp
Learning-Domain: default
Interface: ge-0/2/2.3001
    State:          Up Groups:      0
    Immediate leave: Off
    Router interface: no
```

```
Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2
```

show igmp snooping interface (Group Limit Configured)

```
user@host> show igmp snooping interface instance vpls1
Instance: vpls1

Learning-Domain: default
Interface: ge-1/3/9.0
    State:          Up Groups:      0
    Immediate leave: Off
    Router interface: yes
```

```
Interface: ge-1/3/8.0
  State:          Up Groups:      0
  Immediate leave: Off
  Router interface: yes
  Group limit:    1000
```

```
Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2
```

show igmp snooping membership

Syntax	show igmp snooping membership <brief detail> <bridge-domain <i>bridge-domain-name</i> > <group <i>group-name</i> > <logical-system <i>logical-system-name</i> > <virtual-switch <i>virtual-switch-name</i> > <vlan-id <i>vlan-identifier</i> >
Release Information	Command introduced in Junos OS Release 8.5.
Description	Display IGMP snooping membership information.
Options	<p>none—Display detailed information.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>bridge-domain <i>bridge-domain-name</i>—(Optional) Display information about a particular bridge domain.</p> <p>group <i>group-name</i> —(Optional) Display information about this group address.</p> <p>logical-system <i>logical-system-name</i>—(Optional) Display information about a particular logical system, or type 'all'.</p> <p>virtual-switch <i>virtual-switch-name</i>—(Optional) Display information about a particular virtual switch.</p> <p>vlan-id <i>vlan-identifier</i>—(Optional) Display information about a particular VLAN.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show igmp snooping interface on page 416 • show igmp snooping statistics on page 425 • clear igmp snooping membership on page 414
List of Sample Output	show igmp snooping membership on page 422 show igmp snooping membership (Exclude Mode) on page 423 show igmp snooping membership interface ge-0/1/2.200 on page 423 show igmp snooping membership vlan-id 1 on page 423
Output Fields	Table 12 on page 421 lists the output fields for the show igmp snooping membership command. Output fields are listed in the approximate order in which they appear.

Table 12: show igmp snooping membership Output Fields

Field Name	Field Description	Level of Output
Instance	Routing instance for IGMP snooping.	All levels

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

Field Name	Field Description	Level of Output
Learning Domain	Learning domain for snooping.	All levels
Interface	Interface on which this router is a proxy.	detail
Up Groups	Number of active multicast groups attached to the logical interface.	All levels
Group	Multicast group address in the membership database.	All levels
Group Mode	Mode the SSM group is operating in: Include or Exclude .	All levels
Source	Source address used on queries.	detail
Last reported by	Address of source last replying to the query.	detail
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.	All levels
Timeout	Length of time (in seconds) left until the entry is purged.	detail
Type	Way that the group membership information was learned: <ul style="list-style-type: none"> • Dynamic—Group membership was learned by the IGMP protocol. • Static—Group membership was learned by configuration. 	detail
Include receiver	Source address of receiver included in membership with timeout (in seconds).	detail

Sample Output

show igmp snooping membership

```

user@host> show igmp snooping membership
Instance: vpls2

Learning-Domain: vlan-id 2
Interface: ge-3/0/0.2
Up Groups:      0
Interface: ge-3/1/0.2
Up Groups:      0
Interface: ge-3/1/5.2
Up Groups:      0

Instance: vpls1

Learning-Domain: vlan-id 1
Interface: ge-3/0/0.1
Up Groups:      0
Interface: ge-3/1/0.1
Up Groups:      0
Interface: ge-3/1/5.1
Up Groups:      1

```



```

Group: 225.10.10.1
  Group mode: Exclude
  Source: 0.0.0.0
  Last reported by: 100.6.85.2
  Group timeout: 173 Type: Dynamic

```

show igmp snooping membership (Exclude Mode)

```

user@host> show igmp snooping membership
Instance: vpls2

Learning-Domain: vlan-id 2
Interface: ge-3/0/0.2
Up Groups: 0
Interface: ge-3/1/0.2
Up Groups: 0
Interface: ge-3/1/5.2
Up Groups: 0

Instance: vpls1

Learning-Domain: vlan-id 1
Interface: ge-3/0/0.1
Up Groups: 0
Interface: ge-3/1/0.1
Up Groups: 0
Interface: ge-3/1/5.1
Up Groups: 1
  Group: 225.10.10.1
    Group mode: Exclude
    Source: 0.0.0.0
    Last reported by: 100.6.85.2
    Group timeout: 173 Type: Dynamic

```

show igmp snooping membership interface ge-0/1/2.200

```

user@host> show igmp snooping membership interface ge-0/1/2.200
Instance: bridge-domain bar

Learning-Domain: default
Interface: ge-0/1/2.200
  Group: 225.1.1.1
    Source: 0.0.0.0
    Timeout: 391 Type: Static
  Group: 232.1.1.1
    Source: 192.168.1.1
    Timeout: 0 Type: Static

```

show igmp snooping membership vlan-id 1

```

user@host> show igmp snooping membership vlan-id 1
Instance: vpls2

Instance: vpls1

Learning-Domain: vlan-id 1
Interface: ge-3/0/0.1
Up Groups: 0
Interface: ge-3/1/0.1
Up Groups: 0
Interface: ge-3/1/5.1
Up Groups: 1

```

Group: 225.10.10.1
Group mode: Exclude
Source: 0.0.0.0
Last reported by: 100.6.85.2
Group timeout: 209 Type: Dynamic

show igmp snooping statistics

Syntax	show igmp snooping statistics <brief detail> <bridge-domain <i>bridge-domain-name</i> > <logical-system <i>logical-system-name</i> > <virtual-switch <i>virtual-switch-name</i> > <vlan-id <i>vlan-identifier</i> >
Release Information	Command introduced in Junos OS Release 8.5.
Description	Display IGMP snooping statistics.
Options	<p>none—(Optional) Display detailed information.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>bridge-domain <i>bridge-domain-name</i>—(Optional) Display information about a particular bridge domain.</p> <p>logical-system <i>logical-system-name</i>—(Optional) Display information about a particular logical system, or type 'all'.</p> <p>virtual-switch <i>virtual-switch-name</i>—(Optional) Display information about a particular virtual switch.</p> <p>vlan-id <i>vlan-identifier</i>—(Optional) Display information about a particular VLAN.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show igmp snooping interface on page 416 • show igmp snooping membership on page 421 • clear igmp snooping statistics on page 415
List of Sample Output	show igmp snooping statistics on page 426 show igmp snooping statistics logical-systems all on page 427 show igmp snooping statistics interface (Bridge Domains Configured) on page 428
Output Fields	Table 13 on page 425 lists the output fields for the show igmp snooping statistics command. Output fields are listed in the approximate order in which they appear.

Table 13: show igmp snooping statistics Output Fields

Field Name	Field Description	Level of Output
Routing-instance	Routing instance for IGMP snooping.	All levels
IGMP packet statistics	Heading for IGMP snooping statistics for all interfaces or for the specified interface.	All levels

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

Field Name	Field Description	Level of Output
learning-domain	Appears at end of "IGMP packets statistics" line.	All levels
IGMP Message type	Summary of IGMP statistics: <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. • 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). 	All levels
Received	Number of messages received.	All levels
Sent	Number of messages sent.	All levels
Rx errors	Number of received packets that contained errors.	All levels
IGMP Global Statistics	Summary of IGMP snooping statistics for all interfaces. <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. • Rx non-local—Number of messages received from senders that are not local. 	All levels

Sample Output

show igmp snooping statistics

```

user@host> show igmp snooping statistics
Routing-instance foo

IGMP packet statistics for all interfaces in learning-domain vlan-100

IGMP Message type      Received      Sent  Rx errors

```

Membership Query	89	51	0
V1 Membership Report	0	0	0
DVMRP	0	0	0
PIM V1	0	0	0
Cisco Trace	0	0	0
V2 Membership Report	139	0	0
Group Leave	0	0	0
Domain Wide Report	0	0	0
V3 Membership Report	136	0	0
Other Unknown types			0
IGMP v3 unsupported type			0
IGMP v3 source required for SSM			23
IGMP v3 mode not applicable for SSM			0
IGMP Global Statistics			
Bad Length	0		
Bad Checksum	0		
Rx non-local	0		

Routing-instance bar

IGMP packet statistics for all interfaces in learning-domain vlan-100

IGMP Message type	Received	Sent	Rx errors
Membership Query	89	51	0
V1 Membership Report	0	0	0
DVMRP	0	0	0
PIM V1	0	0	0
Cisco Trace	0	0	0
V2 Membership Report	139	0	0
Group Leave	0	0	0
Domain Wide Report	0	0	0
V3 Membership Report	136	0	0
Other Unknown types			0
IGMP v3 unsupported type			0
IGMP v3 source required for SSM			23
IGMP v3 mode not applicable for SSM			0
IGMP Global Statistics			
Bad Length	0		
Bad Checksum	0		
Rx non-local	0		

show igmp snooping statistics logical-systems all

```
user@host> show igmp snooping statistics logical-systems all
```

```
logical-system: default
Bridge: VPLS-6
IGMP Message type    Received    Sent    Rx errors
Membership Query      0           4         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

Learning-Domain: vlan-id 1041 bridge-domain VS-4-BD-1

IGMP Message type	Received	Sent	Rx errors
Membership Query	0	4	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

Bridge: VPLS-p2mp

IGMP Message type	Received	Sent	Rx errors
Membership Query	0	2	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

Bridge: VS-BD-1

IGMP Message type	Received	Sent	Rx errors
Membership Query	0	6	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

show igmp snooping statistics interface (Bridge Domains Configured)

user@host> show igmp snooping statistics interface

Bridge: bridge-domain1

IGMP interface packet statistics for ge-2/0/8.0

IGMP Message type	Received	Sent	Rx errors
Membership Query	0	2	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

Bridge: bridge-domain2

IGMP interface packet statistics for ge-2/0/8.0

IGMP Message type	Received	Sent	Rx errors
Membership Query	0	2	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

CHAPTER 20

Operational Commands: MLD

- `clear mld membership`
- `clear mld statistics`
- `show mld group`
- `show mld interface`
- `show mld statistics`
- `show multicast pim-to-mld-proxy`

clear mld membership

Syntax	<code>clear mld membership</code> <code><group <i>group-name</i>> <interface <i>interface-name</i>></code> <code><logical-system (all <i>logical-system-name</i>)></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Clear Multicast Listener Discovery (MLD) group membership.
Options	none —Clear all MLD memberships. group <i>group-name</i> —(Optional) Clear MLD membership for the specified group. interface <i>interface-name</i> —(Optional) Clear MLD group membership for the specified interface. logical-system (all <i>logical-system-name</i>) —(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show mld group on page 434
List of Sample Output	clear mld membership on page 432
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear mld membership

```
user@host> clear mld membership
```

clear mld statistics

Syntax	clear mld statistics <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Clear Multicast Listener Discovery (MLD) statistics.
Options	<p>none—(Same as logical-system all) Clear MLD statistics for all interfaces.</p> <p>interface <i>interface-name</i>—(Optional) Clear MLD statistics for 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	clear
Related Documentation	<ul style="list-style-type: none"> • show mld statistics on page 442
List of Sample Output	clear mld statistics on page 433
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear mld statistics

```
user@host> clear mld statistics
```

show mld group

Syntax	show mld group <brief detail> <group-name> <logical-system (all <i>logical-system-name</i>)>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display information about Multicast Listener Discovery (MLD) group membership.
Options	<p>none—Display standard information about all MLD groups.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>group-name—(Optional) Display MLD information about the specified group.</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 mld membership on page 432
List of Sample Output	<p>show mld group (Include Mode) on page 435</p> <p>show mld group (Exclude Mode) on page 436</p> <p>show mld group brief on page 436</p> <p>show mld group detail (Include Mode) on page 436</p> <p>show mld group detail (Exclude Mode) on page 437</p>
Output Fields	Table 14 on page 434 describes the output fields for the show mld group command. Output fields are listed in the approximate order in which they appear.

Table 14: show mld group Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface that received the MLD membership report; local means that the local router joined the group itself.	All levels
Group	Group address.	All levels
Source	Source address.	All levels
Group Mode	Mode the SSM group is operating in: Include or Exclude .	All levels
Last reported by	Address of the host that last reported membership in this group.	All levels

Table 14: show mld 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
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 mld group (Include Mode)

```

user@host> show mld group
Interface: fe-0/1/2.0
  Group: ff02::1:ff05:1a67
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout:      245 Type: Dynamic
  Group: ff02::1:ffa8:c35e
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout:      241 Type: Dynamic
  Group: ff02::2:43e:d7f6
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout:      244 Type: Dynamic
  Group: ff05::2
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout:      244 Type: Dynamic
Interface: local
  Group: ff02::2
    Source: ::
    Last reported by: Local
    Timeout:      0 Type: Dynamic
  Group: ff02::16
    Source: ::
    Last reported by: Local
    Timeout:      0 Type: Dynamic

```

show mld group (Exclude Mode)

```
user@host> show mld group
Interface: ge-0/2/2.0
Interface: ge-0/2/0.0
  Group: ff02::6
    Source: ::
    Last reported by: fe80::21f:12ff:feb6:4b3a
    Timeout:      245 Type: Dynamic
  Group: ff02::16
    Source: ::
    Last reported by: fe80::21f:12ff:feb6:4b3a
    Timeout:      28 Type: Dynamic
Interface: local
  Group: ff02::2
    Source: ::
    Last reported by: Local
    Timeout:      0 Type: Dynamic
  Group: ff02::16
    Source: ::
    Last reported by: Local
    Timeout:      0 Type: Dynamic
```

show mld group brief

The output for the **show mld group brief** command is identical to that for the **show mld group** command. For sample output, see [show mld group \(Include Mode\) on page 435](#) and [show mld group \(Exclude Mode\) on page 436](#).

show mld group detail (Include Mode)

```
user@host> show mld group detail
Interface: fe-0/1/2.0
  Group: ff02::1:ff05:1a67
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout:      224 Type: Dynamic
  Group: ff02::1:ffa8:c35e
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout:      220 Type: Dynamic
  Group: ff02::2:43e:d7f6
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout:      223 Type: Dynamic
  Group: ff05::2
    Group mode: Include
    Source: ::
    Last reported by: fe80::2e0:81ff:fe05:1a67
    Timeout:      223 Type: Dynamic
Interface: so-1/0/1.0
  Group: ff02::2
    Group mode: Include
    Source: ::
    Last reported by: fe80::280:42ff:fe15:f445
    Timeout:      258 Type: Dynamic
Interface: local
```

```

Group: ff02::2
  Group mode: Include
  Source: ::
  Last reported by: Local
  Timeout:      0 Type: Dynamic
Group: ff02::16
  Source: ::
  Last reported by: Local
  Timeout:      0 Type: Dynamic

```

show mld group detail (Exclude Mode)

```

user@host> show mld group detail
Interface: ge-0/2/2.0
Interface: ge-0/2/0.0
  Group: ff02::6
    Group mode: Exclude
    Source: ::
    Source timeout: 0
    Last reported by: fe80::21f:12ff:feb6:4b3a
    Group timeout:   226 Type: Dynamic
  Group: ff02::16
    Group mode: Exclude
    Source: ::
    Source timeout: 0
    Last reported by: fe80::21f:12ff:feb6:4b3a
    Group timeout:   246 Type: Dynamic
Interface: local
  Group: ff02::2
    Group mode: Exclude
    Source: ::
    Source timeout: 0
    Last reported by: Local
    Group timeout:   0 Type: Dynamic
  Group: ff02::16
    Group mode: Exclude
    Source: ::
    Source timeout: 0
    Last reported by: Local
    Group timeout:   0 Type: Dynamic

```

show mld interface

Syntax	show mld interface <brief detail> <interface-name> <logical-system (all <i>logical-system-name</i>)>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display information about Multicast Listener Discovery (MLD)-enabled interfaces.
Options	<p>none—Display standard information about all MLD-enabled interfaces.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>interface-name—(Optional) Display information 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 mld membership on page 432
List of Sample Output	show mld interface on page 440 show mld interface brief on page 440 show mld interface detail on page 441 show mld interface <interface-name> on page 441
Output Fields	<p>Table 15 on page 438 describes the output fields for the show mld interface command. Output fields are listed in the approximate order in which they appear.</p>

Table 15: show mld interface Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface.	All levels
Querier	Address of the router that has been elected to send membership queries.	All levels
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 interface.	All levels
SSM Map Policy	Name of the source-specific multicast (SSM) map policy at the MLD interface.	All levels
Timeout	How long until the MLD querier is declared to be unreachable, in seconds.	All levels
Version	MLD version being used on the interface: 1 or 2.	All levels

Table 15: show mld interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
Groups	Number of groups on the interface.	All levels
Passive	<p>State of the passive mode option:</p> <ul style="list-style-type: none"> • On—Indicates that the router can run IGMP or MLD on the interface but not send or receive control traffic such as IGMP or MLD reports, queries, and leaves. • Off—Indicates that the router can run IGMP or MLD on the interface and send or receive control traffic such as IGMP or MLD reports, queries, and leaves. <p>The passive statement enables you to selectively activate up to two out of a possible three available query or control traffic options. When enabled, the following options appear after the on state declaration:</p> <ul style="list-style-type: none"> • send-general-query—The interface sends general queries. • send-group-query—The interface sends group-specific and group-source-specific queries. • allow-receive—The interface receives control traffic 	All levels
OIF map	Name of the OIF map associated to the interface.	All levels
SSM map	Name of the source-specific multicast (SSM) map used on the interface, if configured.	All levels
Group limit	Maximum number of groups allowed on the interface. Any memberships requested after the limit is reached are rejected.	All levels
Group threshold	<p>Configured threshold at which a warning message is generated.</p> <p>This threshold is based on a percentage of groups received on the interface. If the number of groups received reaches the configured threshold, the device generates a warning message.</p>	All levels
Group log-interval	Time (in seconds) between consecutive log messages.	All levels
Immediate Leave	<p>State of the immediate leave option:</p> <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 multicast listener done message from a host associated with the interface. • Off—Indicates that after receiving a multicast listener done 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

Table 15: show mld interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
Configured Parameters	<p>Information configured by the user.</p> <ul style="list-style-type: none"> • MLD Query Interval (.1 secs)—Interval at which this router sends membership queries when it is the querier. • MLD Query Response Interval (.1 secs)—Time that the router waits for a report in response to a general query. • MLD Last Member Query Interval (.1 secs)—Time that the router waits for a report in response to a group-specific query. • MLD Robustness Count—Number of times the router retries a query. 	All levels
Derived Parameters	<p>Derived information.</p> <ul style="list-style-type: none"> • MLD Membership Timeout (.1 secs)—Timeout period for group membership. If no report is received for these groups before the timeout expires, the group membership will be removed. • MLD Other Querier Present Timeout (.1 secs)—Time that the router waits for the IGMP querier to send a query. 	All levels

Sample Output

show mld interface

```

user@host> show mld interface
Interface: fe-0/0/0
  Querier: None
  State: Up      Timeout:      0    Version:  1    Groups:      0
  SSM Map Policy: ssm-policy-A
Interface: at-0/3/1.0
  Querier: 8038::c0a8:c345
  State: Up      Timeout:    None    Version:  1    Groups:      0
  SSM Map Policy: ssm-policy-B
Interface: fe-1/0/1.0
  Querier: ::192.168.195.73
  State: Up      Timeout:    None    Version:  1    Groups:      3
  SSM Map Policy: ssm-policy-C
  SSM map: ipv6map1
Immediate Leave: On

Configured Parameters:
MLD Query Interval (.1 secs): 1250
MLD Query Response Interval (.1 secs): 100
MLD Last Member Query Interval (.1 secs): 10
MLD Robustness Count: 2

Derived Parameters:
MLD Membership Timeout (.1secs): 2600
MLD Other Querier Present Timeout (.1 secs): 2550

```

show mld interface brief

The output for the **show mld interface brief** command is identical to that for the **show mld interface** command. For sample output, see [show mld interface on page 440](#).

show mld interface detail

The output for the **show mld interface detail** command is identical to that for the **show mld interface** command. For sample output, see [show mld interface on page 440](#).

show mld interface <interface-name>

```
user@host# show mld interface ge-3/2/0.0
Interface: ge-3/2/0.0
Querier: 20.1.1.1
State: Up Timeout:      None Version: 3 Groups:      1
Group limit: 8
Group threshold: 60
Group log-interval: 10
Immediate leave: Off
Promiscuous mode: Off
```

show mld statistics

Syntax	show mld statistics <interface <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display information about Multicast Listener Discovery (MLD) statistics.
Options	<p>none—Display MLD statistics for all interfaces.</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 mld statistics on page 433
List of Sample Output	show mld statistics on page 443 show mld statistics interface on page 444
Output Fields	<p>Table 16 on page 442 describes the output fields for the show mld statistics command. Output fields are listed in the approximate order in which they appear.</p>

Table 16: show mld statistics Output Fields

Field Name	Field Description
Received	Number of received packets.
Sent	Number of transmitted packets.
Rx errors	Number of received packets that contained errors.

Table 16: show mld statistics Output Fields (*continued*)

Field Name	Field Description
MLD Message type	Summary of MLD statistics. <ul style="list-style-type: none"> • Listener Query (v1/v2)—Number of membership queries sent and received. • Listener Report (v1)—Number of version 1 membership reports sent and received. • Listener Done (v1/v2)—Number of Listener Done messages sent and received. • Listener Report (v2)—Number of version 2 membership reports sent and received. • Other Unknown types—Number of unknown message types received. • MLD v2 source required for SSM—Number of MLD version 2 messages received that contained no source. • MLD v2 mode not applicable for SSM—Number of MLD version 2 messages received that did not contain a mode applicable for source-specific multicast (SSM).
MLD Global Statistics	Summary of MLD statistics for all interfaces. <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 an invalid IP checksum. No further classification was performed. • Bad Receive If—Number of messages received on an interface not enabled for MLD. • Rx non-local—Number of messages received from nonlocal senders. • 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 MLD group policy. • Total Interfaces—Number of interfaces configured to support IGMP.

Sample Output

show mld statistics

```

user@host> show mld statistics
MLD packet statistics for all interfaces
MLD Message type      Received      Sent  Rx errors
Listener Query (v1/v2)    0           2      0
Listener Report (v1)      0           0      0
Listener Done (v1/v2)     0           0      0
Listener Report (v2)      0           0      0
Other Unknown types      0           0      0
MLD v2 source required for SSM  2
MLD v2 mode not applicable for SSM 0

MLD Global Statistics
Bad Length              0
Bad Checksum            0
Bad Receive If          0
Rx non-local            0
Timed out               0

```

Rejected Report	0
Total Interfaces	2

show mld statistics interface

```
user@host> show mld statistics interface fe-1/0/1.0
MLD interface packet statistics for fe-1/0/1.0
MLD Message type      Received      Sent  Rx errors
Listener Query (v1/v2)    0           2      0
Listener Report (v1)      0           0      0
Listener Done (v1/v2)     0           0      0
Listener Report (v2)      0           0      0
Other Unknown types              0      0
MLD v2 source required for SSM    2
MLD v2 mode not applicable for SSM 0

MLD Global Statistics
Bad Length                0
Bad Checksum              0
Bad Receive If            0
Rx non-local              0
Timed out                 0
Rejected Report           0
Total Interfaces          2
```

show multicast pim-to-ml-proxy

List of Syntax	Syntax on page 445 Syntax (EX Series Switch and the QFX Series) on page 445
Syntax	<pre>show multicast pim-to-ml-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-ml-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-ml-proxy on page 446 show multicast pim-to-ml-proxy instance on page 446
Output Fields	Table 17 on page 445 describes the output fields for the show multicast pim-to-ml-proxy command. Output fields are listed in the order in which they appear.

Table 17: show multicast pim-to-ml-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
```


CHAPTER 21

Operational Commands: MLD Snooping

- `clear mld snooping membership`
- `clear mld snooping statistics`
- `show mld snooping interface`
- `show mld snooping membership`
- `show mld snooping statistics`
- `show route forwarding-table`
- `show multicast snooping route`
- `show route snooping`

clear mld snooping membership

Syntax	<code>clear mld snooping membership</code> <code><group></code> <code><instance <i>routing-instance</i>></code> <code><interface <i>interface-name</i>></code> <code><qualified-vlan <i>vlan-name</i>></code> <code><vlan <i>vlan-name</i>></code>
Release Information	Command introduced in Junos OS Release 13.3 for EX Series switches. Command introduced in Junos OS Release 14.2 for MX Series routers with MPC.
Description	Clear MLD snooping dynamic group membership information from the multicast forwarding table.
Options	none —Clear all MLD snooping group membership information. group —Clear group membership information for the specified IP address range. instance <i>routing-instance</i> —Clear group membership information for the specified routing instance. interface <i>interface-name</i> —Clear group membership information for the specified interface. qualified-vlan <i>vlan-name</i> —Clear group membership information for the specified qualified VLAN. vlan <i>vlan-name</i> —Clear group membership information for the specified VLAN.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show mld snooping membership on page 453• clear mld snooping statistics on page 449
List of Sample Output	clear mld snooping membership vlan employee-vlan on page 448

Sample Output

clear mld snooping membership vlan employee-vlan

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

clear mld snooping statistics

Syntax	<pre>clear mld snooping statistics <instance <i>routing-instance</i>> <interface <i>interface-name</i>> <qualified-vlan <i>vlan-name</i>> <vlan <i>vlan-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 13.3 for EX Series switches.</p> <p>Command introduced in Junos OS Release 14.2 for MX Series routers with MPC.</p>
Description	Clear MLD snooping statistics.
Options	<p>none—Clear all MLD snooping statistics.</p> <p>instance <i>routing-instance</i>—Clear all MLD snooping statistics for the specified routing instance.</p> <p>interface <i>interface-name</i>—Clear MLD snooping statistics for the specified interface.</p> <p>qualified-vlan <i>vlan-name</i>—Clear MLD snooping statistics for the specified qualified VLAN.</p> <p>vlan <i>vlan-name</i>—Clear MLD snooping statistics for the specified VLAN.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show mld snooping statistics on page 456 • clear mld snooping membership on page 448
List of Sample Output	clear mld snooping statistics on page 449
Sample Output clear mld snooping statistics <pre>user@switch> clear mld snooping statistics</pre>	

show mld snooping interface

Syntax	show mld snooping interface <brief detail> <instance <i>routing-instance</i>> <interface-name> <qualified-vlan <i>vlan-name</i>> <vlan <i>vlan-name</i>>
Release Information	Command introduced in Junos OS Release 13.3 for EX Series switches. Command introduced in Junos OS Release 14.2 for MX Series routers with MPC.
Description	Display MLD snooping information for an interface.
Options	none —Display MLD snooping information for all interfaces on which MLD snooping is enabled. brief detail —(Optional) Display the specified level of output. The default is brief . instance <i>routing-instance</i> —(Optional) Display MLD snooping information for the specified routing instance. interface-name —(Optional) Display MLD snooping information for the specified interface. qualified-vlan <i>vlan-name</i> —(Optional) Display MLD snooping information for the specified qualified VLAN. vlan <i>vlan-name</i> —(Optional) Display MLD snooping information for the specified VLAN.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• clear mld snooping membership on page 448• clear mld snooping statistics on page 449• Verifying MLD Snooping on page 63• Configuring MLD Snooping on a VLAN (CLI Procedure) on page 54
List of Sample Output	show mld snooping interface on page 451 show mld snooping interface ge-0/0/2.0 on page 452 show mld snooping interface brief on page 452 show mld snooping interface detail on page 452
Output Fields	Table 18 on page 451 lists the output fields for the show mld snooping interface command. Output fields are listed in the approximate order in which they appear. Details may differ for EX switches and MX routers.

Table 18: show mld snooping interface Output Fields

Field Name	Field Description	Level of Output
Instance	Routing instance for MLD snooping.	All levels
Learning Domain	Learning domain for MLD snooping.	All levels
Vlan	Name of the VLAN for which MLD snooping is enabled.	All levels
Interface	Name of the interface.	All levels
State	State of the interface: Up or Down .	detail, none
Groups	Number of multicast groups on the interface.	detail, none
Immediate leave	State of the immediate leave option: <ul style="list-style-type: none"> On—Indicates that the MLD querier removes a host from the multicast group as soon as it receives a leave report from a host associated with the interface. Off—Indicates that after receiving a leave report, instead of removing a host from the multicast group immediately, the MLD querier sends a group query to determine if there are any other hosts on that interface still interested in the multicast group. 	detail, none
Router interface	Indicates whether the interface is a multicast router interface: Yes or No .	detail
Configured Parameters	Information configured by the user. <ul style="list-style-type: none"> MLD Query Interval—Interval (in seconds) at which the MLD querier sends membership queries. MLD Query Response Interval—Time (in seconds) that the MLD querier waits for a report in response to a general query. MLD Last Member Query Interval—Time (in seconds) that the MLD querier waits for a report in response to a group-specific query. MLD Robustness Count—Number of times the MLD querier retries a query. 	All levels

Sample Output

show mld snooping interface

```

user@switch> show mld snooping interface
Instance: default-switch

Vlan: v100

Learning-Domain: default
Interface: ge-0/0/1.0
  State:          Up Groups:      1
  Immediate leave: Off
  Router interface: no
Interface: ge-0/0/2.0
  State:          Up Groups:      0
  Immediate leave: Off
  Router interface: no

```

```
Configured Parameters:
MLD Query Interval: 125.0
MLD Query Response Interval: 10.0
MLD Last Member Query Interval: 1.0
MLD Robustness Count: 2
```

show mld snooping interface ge-0/0/2.0

```
user@switch> show mld snooping interface ge-0/0/2.0
Instance: default-switch

Vlan: v100

Learning-Domain: default
Interface: ge-0/0/2.0
  State:          Up Groups:      0
  Immediate leave: Off
  Router interface: no

Configured Parameters:
MLD Query Interval: 125.0
MLD Query Response Interval: 10.0
MLD Last Member Query Interval: 1.0
MLD Robustness Count: 2
```

show mld snooping interface brief

```
user@switch> show mld snooping interface brief
Instance: default-switch

Vlan: v1

Learning-Domain: default
Interface: ge-0/0/1.0
Interface: ge-0/0/2.0

Configured Parameters:
MLD Query Interval: 125.0
MLD Query Response Interval: 10.0
MLD Last Member Query Interval: 1.0
MLD Robustness Count: 2
```

show mld snooping interface detail

The output for the **show mld snooping interface detail** command is identical to that for the **show mld snooping interface** command. For sample output, see [show mld snooping interface on page 451](#).

show mld snooping membership

Syntax	<pre>show mld snooping membership <brief detail> <group> <instance <i>routing-instance</i>> <interface <i>interface-name</i>> <qualified-vlan <i>vlan-name</i>> <vlan <i>vlan-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 13.3 for EX Series switches.</p> <p>Command introduced in Junos OS Release 14.2 for MX Series routers with MPC.</p>
Description	Display the multicast group membership information maintained by MLD snooping.
Options	<p>none—Display the multicast group membership information for all VLANs on which MLD snooping is enabled.</p> <p>brief detail—(Optional) Display the specified level of output. The default is brief.</p> <p>group—Display the multicast group membership information for the specified IP address range.</p> <p>instance <i>routing-instance</i>—(Optional) Display the multicast group membership information for the specified routing instance.</p> <p>interface <i>interface-name</i>—(Optional) Display the multicast group membership for the specified interface.</p> <p>qualified-vlan <i>vlan-name</i>—(Optional) Display the multicast group membership information for the specified qualified VLAN.</p> <p>vlan <i>vlan-name</i>—(Optional) Display the multicast group membership information for the specified VLAN.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show mld snooping interface on page 450 • show mld snooping statistics on page 456 • Verifying MLD Snooping on page 63 • Configuring MLD Snooping on a VLAN (CLI Procedure) on page 54
List of Sample Output	<p>show mld snooping membership on page 454</p> <p>show mld snooping membership brief on page 455</p> <p>show mld snooping membership detail on page 455</p>
Output Fields	<p>Table 18 on page 451 lists the output fields for the show mld snooping membership command. Output fields are listed in the approximate order in which they appear. Details may differ for EX switches and MX routers.</p>

Table 19: show mld snooping membership Output Fields

Field Name	Field Description	Level of Output
Instance	Routing instance for MLD snooping.	All levels
Learning Domain	Learning domain for MLD snooping.	All levels
Vlan	Name of the VLAN for which MLD snooping is enabled.	All levels
Interface	Name of the interface.	All levels
Groups	Number of multicast groups on the interface.	All levels
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"> • Source—Source address for the multicast group. • Last reported by—Last host to report membership for the multicast group. • Group timeout—Time (in seconds) left until a dynamically learned interface is removed from the multicast group if no MLD membership reports are received on the interface. This counter is reset to its maximum value when a membership report is received. • Type—Type of group membership: Dynamic or Static . <ul style="list-style-type: none"> • Dynamic—Host reported the membership. • Static—Membership is configured. 	All levels
Group mode	<p>Mode the source-specific multicast (SSM) group is operating in: Include or Exclude.</p> <ul style="list-style-type: none"> • Include—Multicast traffic is accepted from the configured source address. • Exclude—Multicast traffic is accepted from any address other than the configured source address. 	detail, none

Sample Output

show mld snooping membership

```

user@switch> show mld snooping membership
Instance: default-switch

Vlan: v1

Learning-Domain: default
Interface: ge-0/0/1.0, Groups: 1
  Group: ff03::20
    Group mode: Exclude
    Source: ::
    Last reported by: Local
    Group timeout: 0 Type: Static
Interface: ge-0/0/2.0, Groups: 2
  Group: ff03::10
    Group mode: Exclude
    Source: ::
    Last reported by: Local

```



```

      Group timeout:      0 Type: Static
Group: ff05::1
      Group mode: Exclude
      Source: ::
      Last reported by: fe80::
      Group timeout:     259 Type: Dynamic

```

show mld snooping membership brief

```

user@switch> show mld snooping membership brief
Instance: default-switch

Vlan: v1

Learning-Domain: default
Interface: ge-0/0/1.0, Groups: 1
  Group: ff03::20
    Source: ::
    Last reported by: Local
    Group timeout:    0 Type: Static
Interface: ge-0/0/2.0, Groups: 2
  Group: ff03::10
    Source: ::
    Last reported by: Local
    Group timeout:    0 Type: Static
  Group: ff05::1
    Source: ::
    Last reported by: fe80::
    Group timeout:    259 Type: Dynamic

```

show mld snooping membership detail

The output for the **show mld snooping membership detail** command is identical to that for the **show mld snooping membership** command. For sample output, see [show mld snooping membership on page 454](#).

show mld snooping statistics

Syntax	<pre>show mld statistics <instance <i>routing-instance</i>> <interface <i>interface-name</i>> <qualified-vlan <i>vlan-name</i>> <vlan <i>vlan-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 13.3 for EX Series switches.</p> <p>Command introduced in Junos OS Release 14.2 for MX Series routers with MPC.</p>
Description	Display information about MLD snooping statistics.
Options	<p>none—Display the MLD snooping statistics for all VLANs on which MLD snooping is enabled.</p> <p>instance <i>routing-instance</i>—(Optional) Display MLD snooping statistics for the specified routing instance.</p> <p>interface <i>interface-name</i>—(Optional) Display MLD snooping statistics for the specified interface.</p> <p>qualified-vlan <i>vlan-name</i>—(Optional) Display MLD snooping statistics for the specified qualified VLAN.</p> <p>vlan <i>vlan-name</i>—(Optional) Display MLD snooping statistics for the specified VLAN.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear mld statistics on page 433 • show mld snooping interface on page 450 • Verifying MLD Snooping on page 63 • Configuring MLD Snooping on a VLAN (CLI Procedure) on page 54
List of Sample Output	<p>show mld snooping statistics on page 457</p> <p>show mld snooping statistics interface ge-0/0/1.0 on page 458</p>
Output Fields	<p>Table 16 on page 442 describes the output fields for the show mld snooping statistics command. Output fields are listed in the approximate order in which they appear. Details may differ for EX switches and MX routers.</p>

Table 20: show mld statistics Output Fields

Field Name	Field Description
Received	Number of received packets.
Sent	Number of transmitted packets.

Table 20: show mld statistics Output Fields (*continued*)

Field Name	Field Description
Rx errors	Number of received packets that contained errors.
MLD Message type	Summary of MLD statistics. <ul style="list-style-type: none"> • Listener Query (v1/v2)—Number of membership queries sent and received. • Listener Report (v1)—Number of version 1 membership reports sent and received. • Listener Done (v1/v2)—Number of Listener Done messages sent and received. • Listener Report (v2)—Number of version 2 membership reports sent and received. • Other Unknown types—Number of unknown message types received.
MLD Global Statistics	Summary of MLD statistics for all interfaces. <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 an invalid IP checksum. No further classification was performed. • Bad Receive If—Number of messages received on an interface not enabled for MLD. • Rx non-local—Number of messages received from nonlocal senders. • Timed out—Number of groups that timed out as a result of not receiving an explicit leave message.

Sample Output

show mld snooping statistics

```

user@host> show mld snooping statistics
Vlan: v1
MLD Message type      Received      Sent  Rx errors
Listener Query (v1/v2)    0            4      0
Listener Report (v1)     447          0      0
Listener Done (v1/v2)    0            0      0
Listener Report (v2)     0            0      0
Other Unknown types      0            0      0

Vlan: v2
MLD Message type      Received      Sent  Rx errors
Listener Query (v1/v2)    0            4      0
Listener Report (v1)     154          0      0
Listener Done (v1/v2)    0            0      0
Listener Report (v2)     0            0      0
Other Unknown types      0            0      0

Instance: default-switch
MLD Message type      Received      Sent  Rx errors
Listener Query (v1/v2)    0            8      0
Listener Report (v1)     601          0      0
Listener Done (v1/v2)    0            0      0
Listener Report (v2)     0            0      0
Other Unknown types      0            0      0

```

```
MLD Global Statistics
Bad Length          0
Bad Checksum        0
Bad Receive If      0
Rx non-local        0
Timed out           0
```

show mld snooping statistics interface ge-0/0/1.0

```
user@host> show mld snooping statistics interface ge-0/0/1.0
MLD interface packet statistics for ge-0/0/1.0
MLD Message type      Received      Sent  Rx errors
Listener Query (v1/v2)      0           4       0
Listener Report (v1)        0           0       0
Listener Done (v1/v2)       0           0       0
Listener Report (v2)        0           0       0
Other Unknown types                0       0
```

show route forwarding-table

Syntax	<pre>show route forwarding-table <detail extensive summary> <ccc ccc-interface-name> <destination> <family family-name> <label label> <matching ip_prefix> <multicast> <vpn vpn></pre>
Release Information	Command introduced in Junos OS Release 9.5 for EX Series switches.
Description	Display the Routing Engine's forwarding table, including the network-layer prefixes and their next hops. This command is used to help verify that the routing protocol process has relayed the correction information to the forwarding table. The Routing Engine constructs and maintains one or more routing tables. From the routing tables, the Routing Engine derives a table of active routes, called the forwarding table.
Options	<p>none—Display the routes in the forwarding table.</p> <p>detail extensive summary—(Optional) Display the specified level of output.</p> <p>ccc—(Optional) Display the specified circuit cross-connect interface name for entries to match.</p> <p>destination—(Optional) Display the destination prefix.</p> <p>family family-name—(Optional) Display routing table entries for the specified family: ethernet-switching, inet, inet6, iso, mpls, vlan classification.</p> <p>label label—(Optional) Display route entries for the specified label name.</p> <p>matching ip_prefix—(Optional) Display route entries for the specified IP prefix.</p> <p>multicast—(Optional) Display route entries for multicast routes.</p> <p>vpn vpn—(Optional) Display route entries for the specified VPN.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring MPLS on EX8200 and EX4500 Switches</i> • <i>Configuring MPLS on EX8200 and EX4500 Provider Switches (CLI Procedure)</i>
List of Sample Output	<p>show route forwarding-table on page 461</p> <p>show route forwarding-table summary on page 462</p> <p>show route forwarding-table extensive on page 462</p> <p>show route forwarding-table ccc on page 464</p> <p>show route forwarding-table family (MPLS) on page 464</p>

[show route forwarding-table family \(IPv6\) on page 464](#)

[show route forwarding-table label on page 465](#)

[show route forwarding-table matching on page 465](#)

[show route forwarding-table multicast on page 465](#)

Output Fields [Table 21 on page 460](#) lists the output fields for the **show route forwarding-table** command. Output fields are listed in the approximate order in which they appear. Field names might be abbreviated (as shown in parentheses) when no level of output is specified or when the **detail** keyword is used instead of the **extensive** keyword.

Table 21: show route forwarding-table Output Fields

Field Name	Field Description	Level of Output
Routing table	Name of the routing table (for example, inet , inet6 , mpls).	All levels
Address family	Address family (for example, IP , IPv6 , ISO , MPLS).	All levels
Destination	Destination of the route.	detail , extensive
Route Type (Type)	How the route was placed into the forwarding table. When the detail keyword is used, the route type might be abbreviated (as shown in parentheses): <ul style="list-style-type: none"> • cloned (clon)—(TCP or multicast only) Cloned route. • destination (dest)—Remote addresses directly reachable through an interface. • destination down (iddn)—Destination route for which the interface is unreachable. • interface cloned (ifcl)—Cloned route for which the interface is unreachable. • route down (ifdn)—Interface route for which the interface is unreachable. • ignore (ignr)—Ignore this route. • interface (intf)—Installed as a result of configuring an interface. • permanent (perm)—Routes installed by the kernel when the routing table is initialized. • user—Routes installed by the routing protocol process or as a result of the configuration. 	All levels
Route reference (RtRef)	Number of routes to reference.	detail , extensive
Flags	Route type flags: <ul style="list-style-type: none"> • none—No flags are enabled. • accounting—Route has accounting enabled. • cached—Cache route. • incoming-iface interface-number—Check against incoming interface. • prefix load balance—Load balancing is enabled for this prefix. • sent to PFE—Route has been sent to the Packet Forwarding Engine. • static—Static route. 	extensive
Nexthop	IP address of the next hop to the destination.	detail , extensive

Table 21: show route forwarding-table Output Fields (*continued*)

Field Name	Field Description	Level of Output
Next hop type (Type)	<p>Next-hop type. When the detail keyword is used, the next-hop type might be abbreviated (as indicated in parentheses):</p> <ul style="list-style-type: none"> • broadcast (bcst)—Broadcast. • deny—Deny. • hold—Next hop is waiting to be resolved into a unicast or multicast type. • indexed (idxd)—Indexed next hop. • indirect (indr)—Indirect next hop. • local (locl)—Local address on an interface. • routed multicast (mcrst)—Regular multicast next hop • multicast (mcst)—Wire multicast next hop (limited to the LAN). • multicast discard (mdsc)—Multicast discard. • multicast group (mgrp) —Multicast group member. • receive (recv)—Receive. • reject (rjct)—Discard. An ICMP unreachable message was sent. • resolve (rslv)—Resolving the next hop. • unicast (ucst)—Unicast. • unilist (ulst)—List of unicast next hops. A packet sent to this next hop goes to any next hop in the list. 	detail, extensive
Index	Software index of the next hop that is used to route the traffic for a given prefix.	detail, extensive none
Route interface-index	Logical interface index from which the route is learned. For example, for interface routes, this is the logical interface index of the route itself. For static routes, this field is zero. For routes learned through routing protocols, this is the logical interface index from which the route is learned.	extensive
Reference (NhRef)	Number of routes that refer to this next hop.	none detail, extensive
Next-hop interface (Netif)	Interface used to reach the next hop.	none detail, extensive
Alternate forward nh index	Index number of the alternate next hop interface. Seen with multicast option only.	extensive
Next-hop L3 Interface	The next hop layer 3 interface. This option can be expressed as a VLAN name and is only seen with the multicast option.	extensive
Next-hop L2 Interfaces	The next hop layer 2 interfaces. Seen with multicast option only.	extensive

Sample Output

show route forwarding-table

```

user@switch> show route forwarding-table

Routing table: default.inet

```

Internet:							
Destination	Type	RtRef	Next hop	Type	Index	NhRef	Netif
default	user	2	0:12:f2:21:cf:0	ucst	333	5	me0.0
default	perm	0		rjct	36	2	
0.0.0.0/32	perm	0		dscd	34	1	
2.2.2.0/24	intf	0		rslv	1309	1	ae0.0
2.2.2.0/32	dest	0	2.2.2.0	recv	1307	1	ae0.0
2.2.2.1/32	dest	0	0:21:59:cc:89:c0	ucst	1320	1	ae0.0
2.2.2.2/32	intf	0	2.2.2.2	loc1	1308	2	
2.2.2.2/32	dest	0	2.2.2.2	loc1	1308	2	
2.2.2.255/32	dest	0	2.2.2.255	bcst	1306	1	ae0.0
3.3.3.0/24	intf	0		rslv	1313	1	ae1.0
3.3.3.0/32	dest	0	3.3.3.0	recv	1311	1	ae1.0
3.3.3.1/32	intf	0	3.3.3.1	loc1	1312	2	
3.3.3.1/32	dest	0	3.3.3.1	loc1	1312	2	
3.3.3.2/32	dest	0	0:21:59:cc:89:c1	ucst	1321	24	ae1.0
3.3.3.255/32	dest	0	3.3.3.255	bcst	1310	1	ae1.0
4.4.4.0/24	user	0	3.3.3.2	ucst	1321	24	ae1.0
8.8.8.8/32	user	0	3.3.3.2	ucst	1321	24	ae1.0
9.9.9.9/32	intf	0	9.9.9.9	loc1	1280	1	
10.10.10.10/32	user	0	3.3.3.2	ucst	1321	24	ae1.0
10.93.8.0/21	intf	0		rslv	323	1	me0.0
10.93.8.0/32	dest	0	10.93.8.0	recv	321	1	me0.0
10.93.13.238/32	intf	0	10.93.13.238	loc1	322	2	
10.93.13.238/32	dest	0	10.93.13.238	loc1	322	2	
10.93.15.254/32	dest	0	0:12:f2:21:cf:0	ucst	333	5	me0.0
10.93.15.255/32	dest	0	10.93.15.255	bcst	320	1	me0.0
14.14.14.0/24	ifdn	0		rslv	1319	1	ge-0/0/25.0
14.14.14.0/32	iddn	0	14.14.14.0	recv	1317	1	ge-0/0/25.0
14.14.14.2/32	user	0		rjct	36	2	
14.14.14.2/32	intf	0	14.14.14.2	loc1	1318	2	
14.14.14.2/32	iddn	0	14.14.14.2	loc1	1318	2	
14.14.14.255/32	iddn	0	14.14.14.255	bcst	1316	1	ge-0/0/25.0
224.0.0.0/4	perm	1		mdsc	35	1	
224.0.0.1/32	perm	0	224.0.0.1	mcst	31	3	
224.0.0.5/32	user	1	224.0.0.5	mcst	31	3	
255.255.255.255/32	perm	0		bcst	32	1	

show route forwarding-table summary

```
user@switch> show route forwarding-table summary
```

```
Routing table: default.inet
```

```
Internet:
```

```

user:          6 routes
perm:          5 routes
intf:          8 routes
dest:         12 routes
ifdn:          1 routes
iddn:          3 routes

```

show route forwarding-table extensive

```
user@switch> show route forwarding-table summary
```

```
Routing table: default.inet [Index 0]
```

```
Internet:
```

```
Destination: default
```

```
Route type: user
```

```
Route reference: 2
```

```
Route interface-index: 0
```



```

Flags: sent to PFE, rt nh decoupled
Nexthop: 0:12:f2:21:cf:0
Next-hop type: unicast          Index: 333      Reference: 5
Next-hop interface: me0.0

Destination: default
Route type: permanent
Route reference: 0              Route interface-index: 0
Flags: none
Next-hop type: reject          Index: 36       Reference: 2

Destination: 0.0.0.0/32
Route type: permanent
Route reference: 0              Route interface-index: 0
Flags: sent to PFE
Next-hop type: discard         Index: 34       Reference: 1

Destination: 2.2.2.0/24
Route type: interface
Route reference: 0              Route interface-index: 66
Flags: sent to PFE
Next-hop type: resolve         Index: 1309     Reference: 1
Next-hop interface: ae0.0

Destination: 2.2.2.0/32
Route type: destination
Route reference: 0              Route interface-index: 66
Flags: sent to PFE
Nexthop: 2.2.2.0
Next-hop type: receive         Index: 1307     Reference: 1
Next-hop interface: ae0.0

Destination: 2.2.2.1/32
Route type: destination
Route reference: 0              Route interface-index: 66
Flags: sent to PFE
Nexthop: 0:21:59:cc:89:c0
Next-hop type: unicast         Index: 1320     Reference: 1
Next-hop interface: ae0.0

Destination: 2.2.2.2/32
Route type: interface
Route reference: 0              Route interface-index: 0
Flags: sent to PFE
Nexthop: 2.2.2.2
Next-hop type: local           Index: 1308     Reference: 2

Destination: 2.2.2.2/32
Route type: destination
Route reference: 0              Route interface-index: 66
Flags: none
Nexthop: 2.2.2.2
Next-hop type: local           Index: 1308     Reference: 2

Destination: 2.2.2.255/32
Route type: destination
Route reference: 0              Route interface-index: 66
Flags: sent to PFE
Nexthop: 2.2.2.255
Next-hop type: broadcast       Index: 1306     Reference: 1
Next-hop interface: ae0.0

```

show route forwarding-table ccc

```

user@switch> show route forwarding-table ccc ge-0/0/0.10
Routing table: default.mpls
MPLS:
Destination      Type RtRef Next hop      Type Index NhRef Netif
ge-0/0/0.10      (CCC) user    0 3.3.3.2      Push 300112 1343  2 ae1.0

```

show route forwarding-table family (MPLS)

```

user@switch> show route forwarding-table family mpls

Routing table: default.mpls
MPLS:
Destination      Type RtRef Next hop      Type Index NhRef Netif
default          perm    0
0                user    0      recv    49    3
1                user    0      recv    49    3
2                user    0      recv    49    3
299776           user    0      Pop     1334   2 ge-0/0/0.10
299792           user    0      Pop     1339   2 ge-0/0/0.14
299808           user    0      Pop     1341   2 ge-0/0/0.2
299824           user    0      Pop     1344   2 ge-0/0/0.11
299840           user    0      Pop     1345   2 ge-0/0/0.13
299856           user    0      Pop     1346   2 ge-0/0/0.18
299872           user    0      Pop     1347   2 ge-0/0/0.16
299888           user    0      Pop     1348   2 ge-0/0/0.7
299904           user    0      Pop     1349   2 ge-0/0/0.20
299920           user    0      Pop     1350   2 ge-0/0/0.19
299936           user    0      Pop     1351   2 ge-0/0/0.17
299952           user    0      Pop     1352   2 ge-0/0/0.9
299968           user    0      Pop     1353   2 ge-0/0/0.1
299984           user    0      Pop     1354   2 ge-0/0/0.12
300000           user    0      Pop     1355   2 ge-0/0/0.8
300016           user    0      Pop     1356   2 ge-0/0/0.4
300032           user    0      Pop     1357   2 ge-0/0/0.5
300048           user    0      Pop     1358   2 ge-0/0/0.3
300064           user    0      Pop     1359   2 ge-0/0/0.15
ge-0/0/0.1       (CCC) user    0 3.3.3.2      Push 300064 1340  2 ae1.0
ge-0/0/0.2       (CCC) user    0 3.3.3.2      Push 299872 1328  2 ae1.0
ge-0/0/0.3       (CCC) user    0 3.3.3.2      Push 299792 1323  2 ae1.0
ge-0/0/0.4       (CCC) user    0 3.3.3.2      Push 300016 1337  2 ae1.0
ge-0/0/0.5       (CCC) user    0 3.3.3.2      Push 299824 1325  2 ae1.0
ge-0/0/0.7       (CCC) user    0 3.3.3.2      Push 299920 1331  2 ae1.0
ge-0/0/0.8       (CCC) user    0 3.3.3.2      Push 299840 1326  2 ae1.0
ge-0/0/0.9       (CCC) user    0 3.3.3.2      Push 299888 1329  2 ae1.0
ge-0/0/0.10      (CCC) user    0 3.3.3.2      Push 300112 1343  2 ae1.0
ge-0/0/0.11      (CCC) user    0 3.3.3.2      Push 299776 1322  2 ae1.0
ge-0/0/0.12      (CCC) user    0 3.3.3.2      Push 299952 1333  2 ae1.0
ge-0/0/0.13      (CCC) user    0 3.3.3.2      Push 300096 1342  2 ae1.0
ge-0/0/0.14      (CCC) user    0 3.3.3.2      Push 299984 1335  2 ae1.0
ge-0/0/0.15      (CCC) user    0 3.3.3.2      Push 299936 1332  2 ae1.0
ge-0/0/0.16      (CCC) user    0 3.3.3.2      Push 299808 1324  2 ae1.0
ge-0/0/0.17      (CCC) user    0 3.3.3.2      Push 300000 1336  2 ae1.0
ge-0/0/0.18      (CCC) user    0 3.3.3.2      Push 300032 1338  2 ae1.0
ge-0/0/0.19      (CCC) user    0 3.3.3.2      Push 299904 1330  2 ae1.0
ge-0/0/0.20      (CCC) user    0 3.3.3.2      Push 299856 1327  2 ae1.0

```

show route forwarding-table family (IPv6)

```

user@switch> show route forwarding-table family inet6

```

```

Routing table: default.inet6
Internet6:
Destination      Type RtRef Next hop      Type Index NhRef Netif
default          perm  0              rjct  44    1
::/128           perm  0              dscd  42    1
ff00::/8         perm  0              mdsc  43    1
ff02::1/128      perm  0 ff02::1      mcst  39    1

```

```

Routing table: default-switch.inet6
Internet6:
Destination      Type RtRef Next hop      Type Index NhRef Netif
default          perm  0              rjct  530   1
::/128           perm  0              dscd  528   1
2:1::3a00/312    user  0              indr  131070 2
                  comp  572   1
2:1::3a82/320     user  0              indr  131071 3
                  comp  573   1
2:1::3af0/320     user  0              indr  131071 3
                  comp  573   1
2:1:0:ff00::/56  user  0              mdsc  529   2
ff00::/8         perm  0              mdsc  529   2
ff02::1/128      perm  0 ff02::1      mcst  526   1

```

```

Routing table: __master.anon__.inet6
Internet6:
Destination      Type RtRef Next hop      Type Index NhRef Netif
default          perm  0              rjct  554   1
::/128           perm  0              dscd  552   1
ff00::/8         perm  0              mdsc  553   1
ff02::1/128      perm  0 ff02::1      mcst  550   1

```

show route forwarding-table label

```
user@switch> show route forwarding-table label 29976
```

```

Routing table: default.mpls
MPLS:
Destination      Type RtRef Next hop      Type Index NhRef Netif
299776           user  0              Pop   1334   2 ge-0/0/0.10

```

show route forwarding-table matching

```
user@switch> show route forwarding-table matching 3
```

```

Routing table: default.inet
Internet:

```

show route forwarding-table multicast

```
user@switch> show route forwarding-table multicast
```

```

Routing table: default.inet
Internet:
Destination      Type RtRef Next hop      Type Index NhRef Netif
224.0.0.0/4       perm  1              mdsc  35    1
224.0.0.1/32      perm  0 224.0.0.1      mcst  31    3
224.0.0.5/32      user  1 224.0.0.5      mcst  31    3

```

```

Routing table: __master.anon__.inet
Internet:
Destination      Type RtRef Next hop      Type Index NhRef Netif
224.0.0.0/4       perm  0              mdsc  1289   1

```

```
224.0.0.1/32      perm      0 224.0.0.1      mcst  1285      1
```

```
Routing table: default.inet6
```

```
Internet6:
```

Destination	Type	RtRef	Next hop	Type	Index	NhRef	Netif
ff00::/8	perm	0		mdsc	43	1	
ff02::1/128	perm	0	ff02::1	mcst	39	1	

show multicast snooping route

Syntax show multicast snooping route
 <regexp>
 <active>
 <all>
 <bridge-domain *bridge-domain-name*>
 <brief >
 <control>
 <data>
 <detail >
 <extensive>
 <group *group*>
 <inactive>
 <inet>
 <inet6>
 <instance *instance-name*>
 <logical-system *logical-system-name*>
 <mesh-group *mesh-group-name*>
 <qualified-vlan *vlan-id*>
 <source-prefix *source-prefix*>
 <vlan *vlan-id*>

Release Information Command introduced in Junos OS Release 8.5.
 Support for **control**, **data**, **qualified-vlan** and **vlan** options introduced in Junos OS Release 13.3 for EX Series switches.

Description Display the entries in the IP multicast snooping forwarding table. You can display some of this information with the **show route table inet.1** command.

Options **none**—Display standard information about all entries in the multicast snooping table for all virtual switches and all bridge domains.

active | all | inactive — (Optional) Display all active entries, all entries, or all inactive entries, respectively, in the multicast snooping table.

bridge-domain *bridge-domain*—(Optional) Display the entries for a particular bridge domain.

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

control—(Optional) Display control route entries.

data—(Optional) Display data route entries.

group *group*—(Optional) Display the entries for a particular group.

inet—(Optional) Display IPv4 information.

inet6—(Optional) Display IPv6 information.

instance *instance-name*—(Optional) Display the entries for a multicast instance.

logical-system *logical-system-name*—(Optional) Display information about a particular logical system, or type 'all'.

mesh-group *mesh-group-name*—(Optional) Display the entries for a particular mesh group.

qualified-vlan *vlan-id*—(Optional) Display the entries for a particular qualified VLAN.

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

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

vlan *vlan-id*—(Optional) Display the entries for a particular VLAN.

Required Privilege Level view

List of Sample Output [show multicast snooping route bridge-domain on page 469](#)
[show multicast snooping route instance vs on page 469](#)
[show multicast snooping route extensive on page 469](#)

Output Fields [Table 22 on page 468](#) describes the output fields for the **show multicast snooping route** command. Output fields are listed in the approximate order in which they appear.

Table 22: show multicast snooping route Output Fields

Field Name	Field Description	Level of Output
Next-hop Bulking	Displays whether next-hop bulk updating is ON or OFF (only for routing-instance type of virtual switch or vpls).	All levels
Family	IPv4 address family (INET) or IPv6 address family (INET6).	All levels
Group	Group address.	All levels
Source	Prefix and length of the source as it is in the multicast forwarding table. For (*G) entries, this field is set to "*".	All levels
Routing-instance	Name of the routing instance to which this routing information applies. (Displayed when multicast is configured within a routing instance.)	All levels
Learning Domain	Name of the learning domain to which this routing information applies.	detail extensive
Statistics	Rate at which packets are being forwarded for this source and group entry (in Kbps and pps), and number of packets that have been forwarded to this prefix.	detail extensive
Next-hop ID	Next-hop identifier of the prefix. The identifier is returned by the router's Packet Forwarding Engine and is also displayed in the output of the show multicast nexthops command.	detail extensive
Route state	Whether the group is Active or Inactive .	extensive
Forwarding state	Whether the prefix is Pruned or Forwarding .	extensive

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

Field Name	Field Description	Level of Output
Cache lifetime/timeout	Number of seconds until the prefix is removed from the multicast forwarding table. A value of never indicates a permanent forwarding entry.	extensive

Sample Output

show multicast snooping route bridge-domain

```

user@host> show multicast snooping route bridge-domain br-dom-1 extensive
Family: INET

Group: 232.1.1.1
Source: 192.168.3.100/32
Downstream interface list:
  ge-0/1/0.200
Statistics: 0 kbps, 0 pps, 1 packets
Next-hop ID: 1048577
Route state: Active
Forwarding state: Forwarding
Cache lifetime/timeout: 240 seconds

```

show multicast snooping route instance vs

```

user@host> show multicast snooping route instance vs
Nexthop Bulking: ON

Family: INET

Group: 224.0.0.0
  Bridge-domain: vsid500

Group: 225.1.0.1
  Bridge-domain: vsid500
  Downstream interface list: vsid500
    ge-0/3/8.500 ge-1/1/9.500 ge1/2/5.500

```

show multicast snooping route extensive

```

user@host> show multicast snooping route extensive inet6 group ff03::1
Nexthop Bulking: OFF

Family: INET6
Group: ff03::1/128
Source: ::
Bridge-domain: BD-1
Mesh-group: __all_ces__
Downstream interface list:
  ae0.1 -(562) 1048576
Statistics: 2697 kbps, 3875 pps, 758819039 packets
Next-hop ID: 1048605
Route state: Active
Forwarding state: Forwarding

Group: ff03::1/128
Source: 6666::2/128
Bridge-domain: BD-1
Mesh-group: __all_ces__

```

```
Downstream interface list:
  ae0.1 -(562) 1048576
Statistics: 0 kbps, 0 pps, 0 packets
Next-hop ID: 1048605
Route state: Active
Forwarding state: Forwarding
```


show route snooping

Syntax	<pre>show route snooping <brief detail extensive terse> <all> <best address/prefix> <exact address> <logical-system logical-system-name> <range prefix-range> <summary> <table table-name></pre>
Release Information	<p>Command introduced in Junos OS Release 8.5.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Display the entries in the routing table that were learned from snooping.
Options	<p>none—Display the entries in the routing table that were learned from snooping.</p> <p>brief detail extensive terse—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to brief.</p> <p>all—(Optional) Display all entries, including hidden entries.</p> <p>best address/prefix—(Optional) Display the longest match for the provided address and optional prefix.</p> <p>exact address/prefix—(Optional) Display exact matches for the provided address and optional prefix.</p> <p>logical-system logical-system-name—(Optional) Display information about a particular logical system, or type 'all'.</p> <p>range prefix-range—(Optional) Display information for the provided address range.</p> <p>summary—(Optional) Display route snooping summary statistics.</p> <p>table table-name—(Optional) Display information for the named table.</p>
Required Privilege Level	view
List of Sample Output	<p>show route snooping detail on page 471</p> <p>show route snooping logical-system all on page 472</p>
Output Fields	For information about output fields, see the output field tables for the <i>show route</i> command, the <i>show route detail</i> command, the <i>show route extensive</i> command, or the <i>show route terse</i> command.

Sample Output

show route snooping detail

```
user@host> show route snooping detail
```

```

__+domainAll__.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

224.0.0.2/32 (1 entry, 1 announced)
  *IGMP   Preference: 0
          Next hop type: MultiRecv
          Next-hop reference count: 4
          State: <Active NoReadvrt Int>
          Age: 2:24
          Task: IGMP
          Announcement bits (1): 0-KRT
          AS path: I

224.0.0.22/32 (1 entry, 1 announced)
  *IGMP   Preference: 0
          Next hop type: MultiRecv
          Next-hop reference count: 4
          State: <Active NoReadvrt Int>
          Age: 2:24
          Task: IGMP
          Announcement bits (1): 0-KRT
          AS path: I

__+domainAll__.inet.1: 36 destinations, 36 routes (36 active, 0 holddown, 0 hidden)

224.0.0.0.0.0.0.0/24 (1 entry, 1 announced)
  *Multicast Preference: 180
          Next hop type: Multicast (IPv4), Next hop index: 1048584
          Next-hop reference count: 4
          State: <Active Int>
          Age: 2:24
          Task: MC
          Announcement bits (1): 0-KRT
          AS path: I

<snip>

```

show route snooping logical-system all

```

user@host> show route snooping logical-system all

logical-system: default

inet.1: 20 destinations, 20 routes (20 active, 0 holddown, 0 hidden)
Restart Unsupported
+ = Active Route, - = Last Active, * = Both

0.0,0.1,0.0,232.1.1.65,100.1.1.2/112*[Multicast/180] 00:07:36
      Multicast (IPv4) Composite
0.0,0.1,0.0,232.1.1.66,100.1.1.2/112*[Multicast/180] 00:07:36
      Multicast (IPv4) Composite
0.0,0.1,0.0,232.1.1.67,100.1.1.2/112*[Multicast/180] 00:07:36

<snip>

default-switch.inet.1: 237 dest, 237 rts (237 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

0.15,0.1,0.0,0.0.0.0,0.0.0.0,2/120*[Multicast/180] 00:08:21
      Multicast (IPv4) Composite
0.15,0.1,0.0,0.0.0.0,0.0.0.0,2,17/128*[Multicast/180] 00:08:21

```

Multicast (IPv4) Composite

<snip>

CHAPTER 22

Operational Commands: MSDP

- `show msdp`
- `show msdp source`
- `show msdp source-active`
- `show msdp statistics`
- `show multicast usage`
- `show route table`

show msdp

Syntax	<pre>show msdp <brief detail> <instance <i>instance-name</i>> <logical-system (all <i>logical-system-name</i>)> <peer <i>peer-address</i>></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 12.1 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Display Multicast Source Discovery Protocol (MSDP) information.
Options	<p>none—Display standard MSDP information for all routing instances.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>instance <i>instance-name</i>—(Optional) Display information for the specified instance only.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> <p>peer <i>peer-address</i>—(Optional) Display information about the specified peer only.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show msdp source on page 478 • show msdp source-active on page 480 • show msdp statistics on page 483
List of Sample Output	<p>show msdp on page 477</p> <p>show msdp brief on page 477</p> <p>show msdp detail on page 477</p>
Output Fields	Table 23 on page 476 describes the output fields for the show msdp command. Output fields are listed in the approximate order in which they appear.

Table 23: show msdp Output Fields

Field Name	Field Description	Level of Output
Peer address	IP address of the peer.	All levels
Local address	Local address of the peer.	All levels
State	Status of the MSDP connection: Listen , Established , or Inactive .	All levels
Last up/down	Time at which the most recent peer-state change occurred.	All levels

Table 23: show msdp Output Fields (*continued*)

Field Name	Field Description	Level of Output
Peer-Group	Peer group name.	All levels
SA Count	Number of source-active cache entries advertised by each peer that were accepted, compared to the number that were received, in the format <i>number-accepted/number-received</i> .	All levels
Peer Connect Retries	Number of peer connection retries.	detail
State timer expires	Number of seconds before another message is sent to a peer.	detail
Peer Times out	Number of seconds to wait for a response from the peer before the peer is declared unavailable.	detail
SA accepted	Number of entries in the source-active cache accepted from the peer.	detail
SA received	Number of entries in the source-active cache received by the peer.	detail

Sample Output

show msdp

```

user@host> show msdp
Peer address    Local address  State      Last up/down Peer-Group SA Count
198.32.8.193    198.32.8.195  Established 5d 19:25:44 North23    120/150
198.32.8.194    198.32.8.195  Established 3d 19:27:27 North23    300/345
198.32.8.196    198.32.8.195  Established 5d 19:39:36 North23    10/13
198.32.8.197    198.32.8.195  Established 5d 19:32:27 North23     5/6
198.32.8.198    198.32.8.195  Established 3d 19:33:04 North23   2305/3000

```

show msdp brief

The output for the **show msdp brief** command is identical to that for the **show msdp** command. For sample output, see [show msdp on page 477](#).

show msdp detail

```

user@host> show msdp detail
Peer: 10.255.70.15
Local address: 10.255.70.19
State: Established
Peer Connect Retries: 0
State timer expires: 22
Peer Times out: 49
SA accepted: 0
SA received: 0

```

show msdp source

Syntax	<code>show msdp source</code> <code><instance <i>instance-name</i>></code> <code><logical-system (all <i>logical-system-name</i>)></code> <code><source-address></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 12.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Display multicast sources learned from Multicast Source Discovery Protocol (MSDP).
Options	none —Display standard MSDP source information for all routing instances. instance <i>instance-name</i> —(Optional) Display information for the specified instance only. logical-system (all <i>logical-system-name</i>) —(Optional) Perform this operation on all logical systems or on a particular logical system. source-address —(Optional) IP address and optional prefix length. Display information for the specified source address only.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show msdp on page 476• show msdp source-active on page 480• show msdp statistics on page 483
List of Sample Output	show msdp source on page 479

Output Fields Table 24 on page 479 describes the output fields for the **show msdp source** command. Output fields are listed in the approximate order in which they appear.

Table 24: show msdp source Output Fields

Field Name	Field Description
Source address	IP address of the source.
/Len	Length of the prefix for this IP address.
Type	Discovery method for this multicast source: <ul style="list-style-type: none"> • Configured—Source-active limit explicitly configured for this source. • Dynamic—Source-active limit established when this source was discovered.
Maximum	Source-active limit applied to this source.
Threshold	Source-active threshold applied to this source.
Exceeded	Number of source-active messages received from this source exceeding the established maximum.

Sample Output

show msdp source

```

user@host> show msdp source
Source address /Len  Type      Maximum  Threshold  Exceeded
0.0.0.0       /0    Configured    5         none        0
10.1.0.0      /16   Configured    500       none        0
10.1.1.1      /32   Configured    10000     none        0
10.1.1.2      /32   Dynamic       6936     none        0
10.1.5.5      /32   Dynamic       500       none       123
10.2.1.1      /32   Dynamic        2         none        0

```

show msdp source-active

Syntax	<code>show msdp source-active</code> <code><brief detail></code> <code><group <i>group</i>></code> <code><instance <i>instance-name</i>></code> <code><local></code> <code><logical-system (all <i>logical-system-name</i>)></code> <code><originator <i>originator</i>></code> <code><peer <i>peer-address</i>></code> <code><source <i>source-address</i>></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 12.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Display the Multicast Source Discovery Protocol (MSDP) source-active cache.
Options	none —Display standard MSDP source-active cache information for all routing instances. brief detail —(Optional) Display the specified level of output. group <i>group</i> —(Optional) Display source-active cache information for the specified group. instance <i>instance-name</i> —(Optional) Display information for the specified instance. local —(Optional) Display all source-active caches originated by this router. logical-system (all <i>logical-system-name</i>) —(Optional) Perform this operation on all logical systems or on a particular logical system. originator <i>originator</i> —(Optional) Display information about the peer that originated the source-active cache entries. peer <i>peer-address</i> —(Optional) Display the source-active cache of the specified peer. source <i>source-address</i> —(Optional) Display the source-active cache of the specified source.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show msdp on page 476• show msdp source on page 478• show msdp statistics on page 483
List of Sample Output	show msdp source-active on page 481 show msdp source-active brief on page 482 show msdp source-active detail on page 482 show msdp source-active source on page 482

Output Fields Table 25 on page 481 describes the output fields for the **show msdp source-active** command. Output fields are listed in the approximate order in which they appear.

Table 25: show msdp source-active Output Fields

Field Name	Field Description
Global active source limit exceeded	Number of times all peers have exceeded configured active source limits.
Global active source limit maximum	Configured number of active source messages accepted by the device.
Global active source limit threshold	Configured threshold for applying random early discard (RED) to drop some but not all MSDP active source messages.
Global active source limit log-warning	Threshold at which a warning message is logged (percentage of the number of active source messages accepted by the device).
Global active source limit log interval	Time (in seconds) between consecutive log messages.
Group address	Multicast address of the group.
Source address	IP address of the source.
Peer address	IP address of the peer.
Originator	Router ID configured on the source of the rendezvous point (RP) that originated the message, or the loopback address when the router ID is not configured.
Flags	Flags: Accept , Reject , or Filtered .

Sample Output

show msdp source-active

```

user@host> show msdp source-active
Group address  Source address  Peer address  Originator  Flags
230.0.0.0     192.168.195.46  local        10.255.14.30  Accept
230.0.0.1     192.168.195.46  local        10.255.14.30  Accept
230.0.0.2     192.168.195.46  local        10.255.14.30  Accept
230.0.0.3     192.168.195.46  local        10.255.14.30  Accept
230.0.0.4     192.168.195.46  local        10.255.14.30  Accept

```

show msdp source-active brief

The output for the **show msdp source-active brief** command is identical to that for the **show msdp source-active** command. For sample output, see [show msdp source-active on page 481](#).

show msdp source-active detail

The output for the **show msdp source-active detail** command is identical to that for the **show msdp source-active** command. For sample output, see [show msdp source-active on page 481](#).

show msdp source-active source

```
user@host> show msdp source-active source 192.168.215.246
Global active source limit exceeded: 0
Global active source limit maximum: 25000
Global active source limit threshold: 24000
Global active source limit log-warning: 100
Global active source limit log interval: 0
```

Group address	Source address	Peer address	Originator	Flags
226.2.2.1	192.168.215.246	10.255.182.140	10.255.182.140	Accept
226.2.2.3	192.168.215.246	10.255.182.140	10.255.182.140	Accept
226.2.2.4	192.168.215.246	10.255.182.140	10.255.182.140	Accept
226.2.2.5	192.168.215.246	10.255.182.140	10.255.182.140	Accept
226.2.2.7	192.168.215.246	10.255.182.140	10.255.182.140	Accept
226.2.2.10	192.168.215.246	10.255.182.140	10.255.182.140	Accept
226.2.2.11	192.168.215.246	10.255.182.140	10.255.182.140	Accept
226.2.2.13	192.168.215.246	10.255.182.140	10.255.182.140	Accept
226.2.2.14	192.168.215.246	10.255.182.140	10.255.182.140	Accept
226.2.2.15	192.168.215.246	10.255.182.140	10.255.182.140	Accept

show msdp statistics

Syntax	show msdp statistics <instance <i>instance-name</i> > <logical-system (all <i>logical-system-name</i>)> <peer <i>peer-address</i> >
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 12.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Display statistics about Multicast Source Discovery Protocol (MSDP) peers.
Options	none —Display statistics about all MSDP peers for all routing instances. instance <i>instance-name</i> —(Optional) Display statistics about a specific MSDP instance. logical-system (all <i>logical-system-name</i>) —(Optional) Perform this operation on all logical systems or on a particular logical system. peer <i>peer-address</i> —(Optional) Display statistics about a particular MSDP peer.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>clear msdp statistics</i>
List of Sample Output	show msdp statistics on page 485 show msdp statistics peer on page 485
Output Fields	Table 26 on page 483 describes the output fields for the show msdp statistics command. Output fields are listed in the approximate order in which they appear.

Table 26: show msdp statistics Output Fields

Field Name	Field Description
Global active source limit exceeded	Number of times all peers have exceeded configured active source limits.
Global active source limit maximum	Configured number of active source messages accepted by the device.
Global active source limit threshold	Configured threshold for applying random early discard (RED) to drop some but not all MSDP active source messages.
Global active source limit log-warning	Threshold at which a warning message is logged (percentage of the number of active source messages accepted by the device).
Global active source limit log interval	Time (in seconds) between consecutive log messages.

Table 26: show msdp statistics Output Fields (*continued*)

Field Name	Field Description
Peer	Address of peer.
Last State Change	How long ago the peer state changed.
Last message received from the peer	How long ago the last message was received from the peer.
RPF Failures	Number of reverse path forwarding (RPF) failures.
Remote Closes	Number of times the remote peer closed.
Peer Timeouts	Number of peer timeouts.
SA messages sent	Number of source-active messages sent.
SA messages received	Number of source-active messages received.
SA request messages sent	Number of source-active request messages sent.
SA request messages received	Number of source-active request messages received.
SA response messages sent	Number of source-active response messages sent.
SA response messages received	Number of source-active response messages received.
SA messages with zero Entry Count received	Entry Count is a field within SA message that defines how many source/group tuples are present in the SA message. The counter is incremented each time an SA with an Entry Count of zero is received.
Active source exceeded	Number of times this peer has exceeded configured source-active limits.
Active source Maximum	Configured number of active source messages accepted by this peer.
Active source threshold	Configured threshold on this peer for applying random early discard (RED) to drop some but not all MSDP active source messages.
Active source log-warning	Configured threshold on this peer at which a warning message is logged (percentage of the number of active source messages accepted by the device).
Active source log-interval	Time (in seconds) between consecutive log messages on this peer.
Keepalive messages sent	Number of keepalive messages sent.

Table 26: show msdp statistics Output Fields (*continued*)

Field Name	Field Description
Keepalive messages received	Number of keepalive messages received.
Unknown messages received	Number of unknown messages received.
Error messages received	Number of error messages received.

Sample Output

show msdp statistics

```

user@host> show msdp statistics
Global active source limit exceeded: 0
Global active source limit maximum: 10
Global active source limit threshold: 8
Global active source limit log-warning: 60
Global active source limit log interval: 60

Peer: 10.255.245.39
Last State Change: 11:54:49 (00:24:59)
Last message received from peer: 11:53:32 (00:26:16)
RPF Failures: 0
Remote Closes: 0
Peer Timeouts: 0
SA messages sent: 376
SA messages received: 459
SA messages with zero Entry Count received: 0
SA request messages sent: 0
SA request messages received: 0
SA response messages sent: 0
SA response messages received: 0
Active source exceeded: 0
Active source Maximum: 10
Active source threshold: 8
Active source log-warning: 60
Active source log-interval 120
Keepalive messages sent: 17
Keepalive messages received: 19
Unknown messages received: 0
Error messages received: 0

```

show msdp statistics peer

```

user@host> show msdp statistics peer 10.255.182.140
Peer: 10.255.182.140
  Last State Change: 8:19:23 (00:01:08)
  Last message received from peer: 8:20:05 (00:00:26)
  RPF Failures: 0
  Remote Closes: 0
  Peer Timeouts: 0
  SA messages sent: 17
  SA messages received: 16
  SA request messages sent: 0
  SA request messages received: 0

```

SA response messages sent: 0
SA response messages received: 0
Active source exceeded: 20
Active source Maximum: 10
Active source threshold: 8
Active source log-warning: 60
Active source log-interval: 120
Keepalive messages sent: 0
Keepalive messages received: 0
Unknown messages received: 0
Error messages received: 0

show multicast usage

List of Syntax	Syntax on page 487 Syntax (EX Series Switch and the QFX Series) on page 487
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> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX 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 488 show multicast usage brief on page 488 show multicast usage instance on page 488 show multicast usage detail on page 489
Output Fields	<p>Table 27 on page 488 describes the output fields for the show multicast usage command. Output fields are listed in the approximate order in which they appear.</p>

Table 27: 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 488](#).

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 route table

List of Syntax	Syntax on page 490 Syntax (EX Series Switches) on page 490
Syntax	<code>show route table <i>routing-table-name</i></code> <code><brief detail extensive terse></code> <code><logical-system (all <i>logical-system-name</i>)></code>
Syntax (EX Series Switches)	<code>show route table <i>routing-table-name</i></code> <code><brief detail extensive terse></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display the route entries in a particular routing table.
Options	brief detail extensive terse —(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>routing-table-name</i> —Display route entries for all routing tables whose name begins with this string (for example, inet.0 and inet6.0 are both displayed when you run the show route table inet command).
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show route summary
List of Sample Output	show route table bgp.l2.vpn on page 491 show route table bgp.l3vpn.0 on page 491 show route table bgp.l3vpn.0 detail on page 491 show route table bgp.rtarget.0 (When Proxy BGP Route Target Filtering Is Configured) on page 493 show route table bgp.evpn.0 on page 493 show route table inet.0 on page 493 show route table inet.3 on page 494 show route table inet6.0 on page 494 show route table inet6.3 on page 494 show route table inetflow detail on page 495 show route table l2circuit.0 on page 495 show route table mpls on page 495 show route table mpls extensive on page 496 show route table mpls.0 on page 496 show route table mpls.0 detail (PTX Series) on page 496 show route table mpls.0 extensive (PTX Series) on page 497 show route table mpls.0 (RSVP Route—Transit LSP) on page 498

[show route table vpls_1 detail on page 498](#)
[show route table vpn-a on page 499](#)
[show route table vpn-a.mdt.0 on page 499](#)
[show route table VPN-A detail on page 499](#)
[show route table VPN-AB.inet.0 on page 500](#)
[show route table VPN_blue.mvpn-inet6.0 on page 500](#)
[show route table vrf1.mvpn.0 extensive on page 501](#)
[show route table MVPN.mvpn.0 on page 501](#)
[show route table inetflow detail on page 501](#)

Output Fields For information about output fields, see the output field tables for the **show route** command, the **show route detail** command, the **show route extensive** command, or the **show route terse** command.

Sample Output

show route table bgp.l2vpn

```

user@host> show route table bgp.l2vpn
bgp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.24.1:1:4:1/96
    *[BGP/170] 01:08:58, localpref 100, from 192.168.24.1
    AS path: I
    > to 10.0.16.2 via fe-0/0/1.0, label-switched-path am

```

show route table bgp.l3vpn.0

```

user@host> show route table bgp.l3vpn.0
bgp.l3vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.255.71.15:100:10.255.71.17/32
    *[BGP/170] 00:03:59, MED 1, localpref 100, from
10.255.71.15
    AS path: I
    > via so-2/1/0.0, Push 100020, Push 100011(top)
10.255.71.15:200:10.255.71.18/32
    *[BGP/170] 00:03:59, MED 1, localpref 100, from
10.255.71.15
    AS path: I
    > via so-2/1/0.0, Push 100021, Push 100011(top)

```

show route table bgp.l3vpn.0 detail

```

user@host> show route table bgp.l3vpn.0 detail
bgp.l3vpn.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)

10.255.245.12:1:4.0.0.0/8 (1 entry, 1 announced)
  *BGP Preference: 170/-101
    Route Distinguisher: 10.255.245.12:1
    Source: 10.255.245.12
    Next hop: 192.168.208.66 via fe-0/0/0.0, selected
    Label operation: Push 182449
    Protocol next hop: 10.255.245.12
    Push 182449
    Indirect next hop: 863a630 297

```

```

State: <Active Int Ext>
Local AS: 35 Peer AS: 35
Age: 12:19 Metric2: 1
Task: BGP_35.10.255.245.12+179
Announcement bits (1): 0-BGP.0.0.0.0+179
AS path: 30 10458 14203 2914 3356 I (Atomic) Aggregator: 3356 4.68.0.11

Communities: 2914:420 target:11111:1 origin:56:78
VPN Label: 182449
Localpref: 100
Router ID: 10.255.245.12

10.255.245.12:1:4.17.225.0/24 (1 entry, 1 announced)
*BGP Preference: 170/-101
Route Distinguisher: 10.255.245.12:1
Source: 10.255.245.12
Next hop: 192.168.208.66 via fe-0/0/0.0, selected
Label operation: Push 182465
Protocol next hop: 10.255.245.12
Push 182465
Indirect next hop: 863a8f0 305
State: <Active Int Ext>
Local AS: 35 Peer AS: 35
Age: 12:19 Metric2: 1
Task: BGP_35.10.255.245.12+179
Announcement bits (1): 0-BGP.0.0.0.0+179
AS path: 30 10458 14203 2914 11853 11853 11853 6496 6496 6496 6496 6496 6496 I
Communities: 2914:410 target:12:34 target:11111:1 origin:12:34
VPN Label: 182465
Localpref: 100
Router ID: 10.255.245.12

10.255.245.12:1:4.17.226.0/23 (1 entry, 1 announced)
*BGP Preference: 170/-101
Route Distinguisher: 10.255.245.12:1
Source: 10.255.245.12
Next hop: 192.168.208.66 via fe-0/0/0.0, selected
Label operation: Push 182465
Protocol next hop: 10.255.245.12
Push 182465
Indirect next hop: 86bd210 330
State: <Active Int Ext>
Local AS: 35 Peer AS: 35
Age: 12:19 Metric2: 1
Task: BGP_35.10.255.245.12+179
Announcement bits (1): 0-BGP.0.0.0.0+179
AS path: 30 10458 14203 2914 11853 11853 11853 6496 6496 6496 6496 6496
6496 I
Communities: 2914:410 target:12:34 target:11111:1 origin:12:34
VPN Label: 182465
Localpref: 100
Router ID: 10.255.245.12

10.255.245.12:1:4.17.251.0/24 (1 entry, 1 announced)
*BGP Preference: 170/-101
Route Distinguisher: 10.255.245.12:1
Source: 10.255.245.12
Next hop: 192.168.208.66 via fe-0/0/0.0, selected
Label operation: Push 182465
Protocol next hop: 10.255.245.12

```

```

Push 182465
Indirect next hop: 86bd210 330
State: <Active Int Ext>
Local AS: 35 Peer AS: 35
Age: 12:19 Metric2: 1
Task: BGP_35.10.255.245.12+179
Announcement bits (1): 0-BGP.0.0.0.0+179
AS path: 30 10458 14203 2914 11853 11853 11853 6496 6496 6496 6496 6496

6496 I
Communities: 2914:410 target:12:34 target:11111:1 origin:12:34
VPN Label: 182465
Localpref: 100

```

show route table bgp.rtarget.0 (When Proxy BGP Route Target Filtering Is Configured)

```

user@host> show route table bgp.rtarget.0
bgp.rtarget.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

100:100:100/96
    * [RTarget/5] 00:03:14
      Type Proxy
      for 10.255.165.103
      for 10.255.166.124
      Local

```

show route table bgp.evpn.0

```

user@host> show route table bgp.evpn.0
bgp.evpn.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

2:100.100.100.2:100::0:00:26:88:5f:67:b0/304
    * [BGP/170] 11:00:05, localpref 100, from 100.100.100.2
      AS path: I, validation-state: unverified
      > to 100.1.12.2 via xe-2/2/0.0, label-switched-path R0toR1
2:100.100.100.2:100::0:00:51:51:51:51:51/304
    * [BGP/170] 11:00:05, localpref 100, from 100.100.100.2
      AS path: I, validation-state: unverified
      > to 100.1.12.2 via xe-2/2/0.0, label-switched-path R0toR1
2:100.100.100.3:100::0:00:52:52:52:52:52/304
    * [BGP/170] 10:59:58, localpref 100, from 100.100.100.3
      AS path: I, validation-state: unverified
      > to 100.1.13.3 via ge-2/0/8.0, label-switched-path R0toR2
2:100.100.100.3:100::0:a8:d0:e5:5b:01:c8/304
    * [BGP/170] 10:59:58, localpref 100, from 100.100.100.3
      AS path: I, validation-state: unverified
      > to 100.1.13.3 via ge-2/0/8.0, label-switched-path R0toR2
3:100.100.100.2:100::1000::100.100.100.2/304
    * [BGP/170] 11:00:16, localpref 100, from 100.100.100.2
      AS path: I, validation-state: unverified
      > to 100.1.12.2 via xe-2/2/0.0, label-switched-path R0toR1
3:100.100.100.2:100::2000::100.100.100.2/304
    * [BGP/170] 11:00:16, localpref 100, from 100.100.100.2
      AS path: I, validation-state: unverified
      > to 100.1.12.2 via xe-2/2/0.0, label-switched-path R0toR1

```

show route table inet.0

```

user@host> show route table inet.0

```

```

inet.0: 12 destinations, 12 routes (11 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0      *[Static/5] 00:51:57
                > to 111.222.5.254 via fxp0.0
1.0.0.1/32    *[Direct/0] 00:51:58
                > via at-5/3/0.0
1.0.0.2/32    *[Local/0] 00:51:58
                Local
12.12.12.21/32 *[Local/0] 00:51:57
                Reject
13.13.13.13/32 *[Direct/0] 00:51:58
                > via t3-5/2/1.0
13.13.13.14/32 *[Local/0] 00:51:58
                Local
13.13.13.21/32 *[Local/0] 00:51:58
                Local
13.13.13.22/32 *[Direct/0] 00:33:59
                > via t3-5/2/0.0
127.0.0.1/32  [Direct/0] 00:51:58
                > via lo0.0
111.222.5.0/24 *[Direct/0] 00:51:58
                > via fxp0.0
111.222.5.81/32 *[Local/0] 00:51:58
                Local

```

show route table inet.3

```

user@host> show route table inet.3
inet.3: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

22.0.0.5/32   *[LDP/9] 00:25:43, metric 10, tag 200
                to 1.2.94.2 via lt-1/2/0.49
                > to 1.2.3.2 via lt-1/2/0.23

```

show route table inet6.0

```

user@host> show route table inet6.0
inet6.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Route, * = Both

fec0:0:0:3::/64 *[Direct/0] 00:01:34
>via fe-0/1/0.0

fec0:0:0:3::/128 *[Local/0] 00:01:34
>Local

fec0:0:0:4::/64 *[Static/5] 00:01:34
>to fec0:0:0:3::ffff via fe-0/1/0.0

```

show route table inet6.3

```

user@router> show route table inet6.3
inet6.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

::10.255.245.195/128
                *[LDP/9] 00:00:22, metric 1
                > via so-1/0/0.0
::10.255.245.196/128

```



```
*[LDP/9] 00:00:08, metric 1
> via so-1/0/0.0, Push 100008
```

show route table inetflow detail

```
user@host> show route table inetflow detail
inetflow.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
10.12.44.1,*/48 (1 entry, 1 announced)
    *BGP    Preference: 170/-101
            Next-hop reference count: 2
            State: <Active Ext>
            Local AS: 65002 Peer AS: 65000
            Age: 4
            Task: BGP_65000.10.12.99.5+3792
            Announcement bits (1): 0-Flow
            AS path: 65000 I
            Communities: traffic-rate:0:0
            Validation state: Accept, Originator: 10.12.99.5
            Via: 10.12.44.0/24, Active
            Localpref: 100
            Router ID: 10.255.71.161

10.12.56.1,*/48 (1 entry, 1 announced)
    *Flow    Preference: 5
            Next-hop reference count: 2
            State: <Active>
            Local AS: 65002
            Age: 6:30
            Task: RT Flow
            Announcement bits (2): 0-Flow 1-BGP.0.0.0.0+179
            AS path: I
            Communities: 1:1
```

show route table l2circuit.0

```
user@host> show route table l2circuit.0
l2circuit.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.1.1.195:NoCtrlWord:1:1:Local/96
    *[L2CKT/7] 00:50:47
    > via so-0/1/2.0, Push 100049
    via so-0/1/3.0, Push 100049
10.1.1.195:NoCtrlWord:1:1:Remote/96
    *[LDP/9] 00:50:14
    Discard
10.1.1.195:CtrlWord:1:2:Local/96
    *[L2CKT/7] 00:50:47
    > via so-0/1/2.0, Push 100049
    via so-0/1/3.0, Push 100049
10.1.1.195:CtrlWord:1:2:Remote/96
    *[LDP/9] 00:50:14
    Discard
```

show route table mpls

```
user@host> show route table mpls
mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0                *[MPLS/0] 00:13:55, metric 1
                  Receive
```

```

1          *[MPLS/0] 00:13:55, metric 1
           Receive
2          *[MPLS/0] 00:13:55, metric 1
           Receive
1024       *[VPN/0] 00:04:18
           to table red.inet.0, Pop

```

show route table mpls extensive

```

user@host> show route table mpls extensive
100000 (1 entry, 1 announced)
TSI:
KRT in-kernel 100000 /36 -> {so-1/0/0.0}
    *LDP    Preference: 9
           Next hop: via so-1/0/0.0, selected
           Pop
           State: <Active Int>
           Age: 29:50      Metric: 1
           Task: LDP
           Announcement bits (1): 0-KRT
           AS path: I
           Prefixes bound to route: 10.0.0.194/32

```

show route table mpls.0

```

user@host> show route table mpls.0
mpls.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0          *[MPLS/0] 00:45:09, metric 1
           Receive
1          *[MPLS/0] 00:45:09, metric 1
           Receive
2          *[MPLS/0] 00:45:09, metric 1
           Receive
100000     *[L2VPN/7] 00:43:04
           > via so-0/1/0.1, Pop
100001     *[L2VPN/7] 00:43:03
           > via so-0/1/0.2, Pop      Offset: 4
100002     *[LDP/9] 00:43:22, metric 1
           via so-0/1/2.0, Pop
           > via so-0/1/3.0, Pop
100002(S=0) *[LDP/9] 00:43:22, metric 1
           via so-0/1/2.0, Pop
           > via so-0/1/3.0, Pop
100003     *[LDP/9] 00:43:22, metric 1
           > via so-0/1/2.0, Swap 100002
           via so-0/1/3.0, Swap 100002
100004     *[LDP/9] 00:43:16, metric 1
           via so-0/1/2.0, Swap 100049
           > via so-0/1/3.0, Swap 100049
so-0/1/0.1 *[L2VPN/7] 00:43:04
           > via so-0/1/2.0, Push 100001, Push 100049(top)
           via so-0/1/3.0, Push 100001, Push 100049(top)
so-0/1/0.2 *[L2VPN/7] 00:43:03
           via so-0/1/2.0, Push 100000, Push 100049(top) Offset: -4
           > via so-0/1/3.0, Push 100000, Push 100049(top) Offset: -4

```

show route table mpls.0 detail (PTX Series)

```

user@host> show route table mpls.0 detail

```

```

ge-0/0/2.600 (1 entry, 1 announced)
  *L2VPN Preference: 7
    Next hop type: Indirect
    Address: 0x9438f34
    Next-hop reference count: 2
    Next hop type: Router, Next hop index: 567
    Next hop: 3.0.0.1 via ge-0/0/1.0, selected
    Label operation: Push 299808
    Label TTL action: prop-ttl
    Load balance label: Label 299808:None;
    Session Id: 0x1
    Protocol next hop: 10.255.255.1
    Label operation: Push 299872 Offset: 252
    Label TTL action: no-prop-ttl
    Load balance label: Label 299872:Flow label PUSH;
    Composite next hop: 0x9438ed8 570 INH Session ID: 0x2
    Indirect next hop: 0x9448208 262142 INH Session ID: 0x2
    State: <Active Int>
    Age: 21 Metric2: 1
    Validation State: unverified
    Task: Common L2 VC
    Announcement bits (2): 0-KRT 2-Common L2 VC
    AS path: I

```

show route table mpls.0 extensive (PTX Series)

```

user@host> show route table mpls.0 extensive
ge-0/0/2.600 (1 entry, 1 announced)
TSI:
KRT in-kernel ge-0/0/2.600.0 /32 -> {composite(570)}
  *L2VPN Preference: 7
    Next hop type: Indirect
    Address: 0x9438f34
    Next-hop reference count: 2
    Next hop type: Router, Next hop index: 567
    Next hop: 3.0.0.1 via ge-0/0/1.0, selected
    Label operation: Push 299808
    Label TTL action: prop-ttl
    Load balance label: Label 299808:None;
    Session Id: 0x1
    Protocol next hop: 10.255.255.1
    Label operation: Push 299872 Offset: 252
    Label TTL action: no-prop-ttl
    Load balance label: Label 299872:Flow label PUSH;
    Composite next hop: 0x9438ed8 570 INH Session ID: 0x2
    Indirect next hop: 0x9448208 262142 INH Session ID: 0x2
    State: <Active Int>
    Age: 47 Metric2: 1
    Validation State: unverified
    Task: Common L2 VC
    Announcement bits (2): 0-KRT 2-Common L2 VC
    AS path: I
    Composite next hops: 1
      Protocol next hop: 10.255.255.1 Metric: 1
      Label operation: Push 299872 Offset: 252
      Label TTL action: no-prop-ttl
      Load balance label: Label 299872:Flow label PUSH;
      Composite next hop: 0x9438ed8 570 INH Session ID: 0x2
      Indirect next hop: 0x9448208 262142 INH Session ID: 0x2
      Indirect path forwarding next hops: 1
        Next hop type: Router

```

```

Next hop: 3.0.0.1 via ge-0/0/1.0
Session Id: 0x1
10.255.255.1/32 Originating RIB: inet.3
Metric: 1                               Node path count: 1
Forwarding nexthops: 1
Nexthop: 3.0.0.1 via ge-0/0/1.0

```

show route table mpls.0 (RSVP Route—Transit LSP)

In the sample output, the 1 in [RSVP/7/1] indicates the secondary preference value. The secondary preference value becomes significant when multiple RSVP LSPs of different types are signaled to the destination. The possible values of RSVP secondary preferences are:

1—Normal Point-to-Point RSVP-TE LSP

2—Point-to-Multipoint (P2MP) RSVP-TE LSP

3—Dynamic RSVP-TE LSP

```
user@host> show route table mpls.0
```

```
mpls.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
```

```

0          *[MPLS/0] 00:37:31, metric 1
            Receive
1          *[MPLS/0] 00:37:31, metric 1
            Receive
2          *[MPLS/0] 00:37:31, metric 1
            Receive
13         *[MPLS/0] 00:37:31, metric 1
            Receive
300352     *[RSVP/7/1] 00:08:00, metric 1
            > to 8.64.0.106 via ge-1/0/1.0, label-switched-path lsp1_p2p
300352(S=0) *[RSVP/7/1] 00:08:00, metric 1
            > to 8.64.0.106 via ge-1/0/1.0, label-switched-path lsp1_p2p
300384     *[RSVP/7/2] 00:05:20, metric 1
            > to 8.64.1.106 via ge-1/0/0.0, Pop
300384(S=0) *[RSVP/7/2] 00:05:20, metric 1
            > to 8.64.1.106 via ge-1/0/0.0, Pop

```

show route table vpls_1 detail

```
user@host> show route table vpls_1 detail
```

```
vpls_1.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Restart Complete
```

```

1.1.1.11:1000:1:1/96 (1 entry, 1 announced)
*L2VPN Preference: 170/-1
Receive table: vpls_1.l2vpn.0
Next-hop reference count: 2
State: <Active Int Ext>
Age: 4:29:47 Metric2: 1
Task: vpls_1-l2vpn
Announcement bits (1): 1-BGP.0.0.0.0+179
AS path: I
Communities: Layer2-info: encaps:VPLS, control flags:Site-Down
Label-base: 800000, range: 8, status-vector: 0xFF

```

show route table vpn-a

```

user@host> show route table vpn-a
vpn-a.12vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)

+ = Active Route, - = Last Active, * = Both
192.168.16.1:1:1:1/96
    *[VPN/7] 05:48:27
    Discard
192.168.24.1:1:2:1/96
    *[BGP/170] 00:02:53, localpref 100, from 192.168.24.1
    AS path: I
    > to 10.0.16.2 via fe-0/0/1.0, label-switched-path am
192.168.24.1:1:3:1/96
    *[BGP/170] 00:02:53, localpref 100, from 192.168.24.1
    AS path: I
    > to 10.0.16.2 via fe-0/0/1.0, label-switched-path am

```

show route table vpn-a.mdt.0

```

user@host> show route table vpn-a.mdt.0
vpn-a.mdt.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1:1:0:10.255.14.216:232.1.1.1/144
    *[MVPN/70] 01:23:05, metric2 1
    Indirect
1:1:1:10.255.14.218:232.1.1.1/144
    *[BGP/170] 00:57:49, localpref 100, from 10.255.14.218
    AS path: I
    > via so-0/0/0.0, label-switched-path r0e-to-r1
1:1:2:10.255.14.217:232.1.1.1/144
    *[BGP/170] 00:57:49, localpref 100, from 10.255.14.217
    AS path: I
    > via so-0/0/1.0, label-switched-path r0-to-r2

```

show route table VPN-A detail

```

user@host> show route table VPN-A detail
VPN-AB.inet.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
10.255.179.9/32 (1 entry, 1 announced)
    *BGP Preference: 170/-101
    Route Distinguisher: 10.255.179.13:200
    Next hop type: Indirect
    Next-hop reference count: 5
    Source: 10.255.179.13
    Next hop type: Router, Next hop index: 732
    Next hop: 10.39.1.14 via fe-0/3/0.0, selected
    Label operation: Push 299824, Push 299824(top)
    Protocol next hop: 10.255.179.13
    Push 299824
    Indirect next hop: 8f275a0 1048574
    State: (Secondary Active Int Ext)
    Local AS: 1 Peer AS: 1
    Age: 3:41:06 Metric: 1 Metric2: 1
    Task: BGP_1.10.255.179.13+64309
    Announcement bits (2): 0-KRT 1-BGP RT Background
    AS path: I
    Communities: target:1:200 rte-type:0.0.0.0:1:0
    Import Accepted
    VPN Label: 299824 TTL Action: vrf-ttl-propagate

```

```

Localpref: 100
Router ID: 10.255.179.13
Primary Routing Table bgp.13vpn.0

```

show route table VPN-AB.inet.0

```

user@host> show route table VPN-AB.inet.0
VPN-AB.inet.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.0/30      *[OSPF/10] 00:07:24, metric 1
                  > via so-7/3/1.0
10.39.1.4/30      *[Direct/0] 00:08:42
                  > via so-5/1/0.0
10.39.1.6/32      *[Local/0] 00:08:46
                  Local
10.255.71.16/32   *[Static/5] 00:07:24
                  > via so-2/0/0.0
10.255.71.17/32   *[BGP/170] 00:07:24, MED 1, localpref 100, from
10.255.71.15
                  AS path: I
                  > via so-2/1/0.0, Push 100020, Push 100011(top)
10.255.71.18/32   *[BGP/170] 00:07:24, MED 1, localpref 100, from
10.255.71.15
                  AS path: I
                  > via so-2/1/0.0, Push 100021, Push 100011(top)
10.255.245.245/32 *[BGP/170] 00:08:35, localpref 100
                  AS path: 2 I
                  > to 10.39.1.5 via so-5/1/0.0
10.255.245.246/32 *[OSPF/10] 00:07:24, metric 1
                  > via so-7/3/1.0

```

show route table VPN_blue.mvpn-inet6.0

```

user@host> show route table VPN_blue.mvpn-inet6.0
vpn_blue.mvpn-inet6.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1::10.255.2.202:65535:10.255.2.202/432
                  *[BGP/170] 00:02:37, localpref 100, from 10.255.2.202
                  AS path: I
                  > via so-0/1/3.0
1::10.255.2.203:65535:10.255.2.203/432
                  *[BGP/170] 00:02:37, localpref 100, from 10.255.2.203
                  AS path: I
                  > via so-0/1/0.0
1::10.255.2.204:65535:10.255.2.204/432
                  *[MVPN/70] 00:57:23, metric2 1
                  Indirect
5::10.255.2.202:65535:128::192.168.90.2:128:ffff::1/432
                  *[BGP/170] 00:02:37, localpref 100, from 10.255.2.202
                  AS path: I
                  > via so-0/1/3.0
6::10.255.2.203:65535:65000:128::10.12.53.12:128:ffff::1/432
                  *[PIM/105] 00:02:37
                  Multicast (IPv6)
7::10.255.2.202:65535:65000:128::192.168.90.2:128:ffff::1/432
                  *[MVPN/70] 00:02:37, metric2 1
                  Indirect

```

show route table vrf1.mvpn.0 extensive

```

user@host> show route table vrf1.mvpn.0 extensive
1:10.255.50.77:1:10.255.50.77/240 (1 entry, 1 announced)
    *MVPN    Preference: 70
              PMSI: Flags 0x0: Label 0: RSVP-TE:
Session_13[10.255.50.77:0:25624:10.255.50.77]
    Next hop type: Indirect
    Address: 0xbb2c944
    Next-hop reference count: 360
    Protocol next hop: 10.255.50.77
    Indirect next hop: 0x0 - INH Session ID: 0x0
    State: <Active Int Ext>
    Age: 53:03      Metric2: 1
    Validation State: unverified
    Task: mvpn global task
    Announcement bits (3): 0-PIM.vrf1 1-mvpn global task 2-rt-export

    AS path: I

```

show route table MVPN.mvpn.0

Starting in Junos OS Release 15.1, multicast routes on the locally originated type 7 customer multicast routes are added exclusively by PIM. The functionality of the BGP-MVPN service (which, internally, depends on contributions of state from both the MVPN and PIM protocol components of Junos OS) remains unchanged. MVPN, however, no longer appears as the originator of the locally advertised route. Routes advertised by remote PEs are, as usual, always learned locally from their respective [BGP/...] protocol.

```

user@host> show route table MVPN.mvpn.0
MVPN.mvpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

7:10.255.2.202:65535:65000:128:::192.168.90.2:128:ffff::1/432
    * [PIM/70] 00:02:37, metric2 1
    Indirect
5:100:32:192.168.1.9:32:239.1.1.1/240
    * [PIM/105] 01:51:21
    Multicast (IPv4)
7:100:1:100.32.192.168.5:32:237.1.1.1/240
    * [PIM/105] 01:51:21
    Multicast (IPv4)

```

show route table inetflow detail

```

user@host> show route table inetflow detail
inetflow.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
10.12.44.1,*/48 (1 entry, 1 announced)
    *BGP      Preference: 170/-101
              Next-hop reference count: 2
              State: <Active Ext>
              Local AS: 65002 Peer AS: 65000
              Age: 4
              Task: BGP_65000.10.12.99.5+3792
              Announcement bits (1): 0-Flow
              AS path: 65000 I
              Communities: traffic-rate:0:0
              Validation state: Accept, Originator: 10.12.99.5
              Via: 10.12.44.0/24, Active
              Localpref: 100

```

```

Router ID: 10.255.71.161

10.12.56.1,*/48 (1 entry, 1 announced)
  *Flow Preference: 5
    Next-hop reference count: 2
    State: <Active>
    Local AS: 65002
    Age: 6:30
    Task: RT Flow
    Announcement bits (2): 0-Flow 1-BGP.0.0.0.0+179
    AS path: I
    Communities: 1:1

user@PE1> show route table green.l2vpn.0 (VPLS Multihoming with FEC 129)
green.l2vpn.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1.1.1.2:100:1.1.1.2/96 AD
    *[VPLS/170] 1d 03:11:03, metric2 1
    Indirect
1.1.1.4:100:1.1.1.4/96 AD
    *[BGP/170] 1d 03:11:02, localpref 100, from 1.1.1.4
    AS path: I, validation-state: unverified
    > via ge-1/2/1.5
1.1.1.2:100:1:0/96 MH
    *[VPLS/170] 1d 03:11:03, metric2 1
    Indirect
1.1.1.4:100:1:0/96 MH
    *[BGP/170] 1d 03:11:02, localpref 100, from 1.1.1.4
    AS path: I, validation-state: unverified
    > via ge-1/2/1.5
1.1.1.4:NoCtrlWord:5:100:100:1.1.1.2:1.1.1.4/176
    *[VPLS/7] 1d 03:11:02, metric2 1
    > via ge-1/2/1.5
1.1.1.4:NoCtrlWord:5:100:100:1.1.1.4:1.1.1.2/176
    *[LDP/9] 1d 03:11:02
    Discard

user@host> show route table red extensive
red.inet.0: 364481 destinations, 714087 routes (364480 active, 48448 holddown, 1
hidden)
22.0.0.0/32 (3 entries, 1 announced)
  State: <OnList CalcForwarding>
TSI:
KRT in-kerne1 22.0.0.0/32 -> {composite(1048575)} Page 0 idx 1 Type 1 val 0x934342c

  Nexthop: Self
  AS path: [2] I
  Communities: target:2:1
Path 22.0.0.0 from 2.3.0.0 Vector len 4. Val: 1
  @BGP Preference: 170/-1
    Route Distinguisher: 2:1
    Next hop type: Indirect
    Address: 0x258059e4
    Next-hop reference count: 2
    Source: 2.2.0.0
    Next hop type: Router
    Next hop: 10.1.1.1 via ge-1/1/9.0, selected
    Label operation: Push 707633
    Label TTL action: prop-ttl
    Session Id: 0x17d8

```



```

Protocol next hop: 2.2.0.0
Push 16
Composite next hop: 0x25805988 - INH Session ID: 0x193c
Indirect next hop: 0x23eea900 - INH Session ID: 0x193c
State: <Secondary Active Int Ext ProtectionPath ProtectionCand>
Local AS:      2 Peer AS:      2
Age: 23        Metric2: 35
Validation State: unverified
Task: BGP_2.2.2.0.0+34549
AS path: I
Communities: target:2:1
Import Accepted
VPN Label: 16
Localpref: 0
Router ID: 2.2.0.0
Primary Routing Table bgp.13vpn.0
Composite next hops: 1
  Protocol next hop: 2.2.0.0 Metric: 35
  Push 16
  Composite next hop: 0x25805988 - INH Session ID: 0x193c
  Indirect next hop: 0x23eea900 - INH Session ID: 0x193c
  Indirect path forwarding next hops: 1
    Next hop type: Router
    Next hop: 10.1.1.1 via ge-1/1/9.0
    Session Id: 0x17d8
  2.2.0.0/32 Originating RIB: inet.3
  Metric: 35                      Node path count: 1
  Forwarding nexthops: 1
    Nexthop: 10.1.1.1 via ge-1/1/9.0
BGP Preference: 170/-1
Route Distinguisher: 2:1
Next hop type: Indirect
Address: 0x9347028
Next-hop reference count: 3
Source: 2.3.0.0
Next hop type: Router, Next hop index: 702
Next hop: 10.1.4.2 via ge-1/0/0.0, selected
Label operation: Push 634278
Label TTL action: prop-ttl
Session Id: 0x17d9
Protocol next hop: 2.3.0.0
Push 16
Composite next hop: 0x93463a0 1048575 INH Session ID: 0x17da
Indirect next hop: 0x91e8800 1048574 INH Session ID: 0x17da
State: <Secondary NotBest Int Ext ProtectionPath ProtectionCand>

Inactive reason: Not Best in its group - IGP metric
Local AS:      2 Peer AS:      2
Age: 3:34      Metric2: 70
Validation State: unverified
Task: BGP_2.2.3.0.0+32805
Announcement bits (2): 0-KRT 1-BGP_RT_Background
AS path: I
Communities: target:2:1
Import Accepted
VPN Label: 16
Localpref: 0
Router ID: 2.3.0.0
Primary Routing Table bgp.13vpn.0
Composite next hops: 1
  Protocol next hop: 2.3.0.0 Metric: 70

```

```

                                Push 16
                                Composite next hop: 0x93463a0 1048575 INH Session ID:
0x17da
                                Indirect next hop: 0x91e8800 1048574 INH Session ID:
0x17da
                                Indirect path forwarding next hops: 1
                                    Next hop type: Router
                                    Next hop: 10.1.4.2 via ge-1/0/0.0
                                    Session Id: 0x17d9
                                2.3.0.0/32 Originating RIB: inet.3
                                    Metric: 70                                Node path count: 1
                                    Forwarding nexthops: 1
                                        Nexthop: 10.1.4.2 via ge-1/0/0.0
#Multipath Preference: 255
    Next hop type: Indirect
    Address: 0x24afca30
    Next-hop reference count: 1
    Next hop type: Router
    Next hop: 10.1.1.1 via ge-1/1/9.0, selected
    Label operation: Push 707633
    Label TTL action: prop-ttl
    Session Id: 0x17d8
    Next hop type: Router, Next hop index: 702
    Next hop: 10.1.4.2 via ge-1/0/0.0
    Label operation: Push 634278
    Label TTL action: prop-ttl
    Session Id: 0x17d9
    Protocol next hop: 2.2.0.0
    Push 16
    Composite next hop: 0x25805988 - INH Session ID: 0x193c
    Indirect next hop: 0x23eea900 - INH Session ID: 0x193c Weight 0x1

    Protocol next hop: 2.3.0.0
    Push 16
    Composite next hop: 0x93463a0 1048575 INH Session ID: 0x17da
    Indirect next hop: 0x91e8800 1048574 INH Session ID: 0x17da Weight
0x4000
    State: <ForwardingOnly Int Ext>
    Inactive reason: Forwarding use only
    Age: 23                                Metric2: 35
    Validation State: unverified
    Task: RT
    AS path: I
    Communities: target:2:1

```

CHAPTER 23

Operational Commands: PIM

- `clear pim join`
- `clear pim join-distribution`
- `clear pim register`
- `clear pim statistics`
- `request pim multicast-tunnel rebalance`
- `show pim bidirectional df-election`
- `show pim bidirectional df-election interface`
- `show pim bootstrap`
- `show pim interfaces`
- `show pim join`
- `show pim neighbors`
- `show pim rps`
- `show pim source`
- `show pim statistics`

clear pim join

List of Syntax [Syntax on page 506](#)
 [Syntax \(EX Series Switch and the QFX Series\) on page 506](#)

Syntax clear pim join
 <group-address>
 <bidirectional | dense | sparse>
 <exact>
 <inet | inet6>
 <instance instance-name>
 <logical-system (all | logical-system-name)>
 <rp ip-address/prefix | source ip-address/prefix>
 <sg | star-g>

Syntax (EX Series Switch and the QFX Series) clear pim join
 <group-address>
 <dense | sparse>
 <exact>
 <inet | inet6>
 <instance instance-name>
 <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.
 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.
 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 Clear the Protocol Independent Multicast (PIM) join and prune states.

Options **none**—Clear the PIM join and prune states for all groups, family addresses, and instances.

group-address—(Optional) Clear the PIM join and prune states for a group address.

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

exact—(Optional) Clear only the group that exactly matches the specified group address.

inet | inet6—(Optional) Clear the PIM entries for IPv4 or IPv6 family addresses, respectively.

instance instance-name—(Optional) Clear the entries 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.

rp ip-address/prefix | source ip-address/prefix—(Optional) Clear 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) Clear PIM (S,G) or (*,G) entries.

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

- [show pim join on page 527](#)

List of Sample Output

- [clear pim join on page 507](#)
- [clear pim join inet6 on page 507](#)
- [clear pim join inet6 star-g on page 507](#)

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
Cleared 8 Join/Prune states
```

`clear pim join inet6`

```
user@host> clear pim join inet6
Cleared 4 Join/Prune states
```

`clear pim join inet6 star-g`

```
user@host> clear pim join inet6 star-g
Cleared 1 Join/Prune states
```

clear pim join-distribution

Syntax	<code>clear pim join-distribution</code> <code><instance <i>instance-name</i>></code> <code><logical-system (all <i>logical-system-name</i>)></code>
Release Information	Command introduced in Junos OS Release 10.0.
Description	<p>Redistribute the Protocol Independent Multicast (PIM) join states.</p> <p>You can find out if there are multiple paths available for a source (for example, an RP) with the output of the show pim source command.</p> <p>When you include the join-load-balance statement in the configuration, the PIM join states are distributed evenly on available equal-cost multipath links. When an upstream neighbor link fails, Junos OS redistributes the PIM join states to the remaining links. However, when new links are added or the failed link is restored, the existing PIM joins are not redistributed to the new link. New flows will be distributed to the new links. However, in a network without new joins and prunes, the new link is not used for multicast traffic. The clear pim join-distribution command redistributes the existing flows to the new upstream neighbors. Redistributing the existing flows causes traffic to be disrupted, so we recommend that you run the clear pim join-distribution command during a maintenance window.</p>
Options	<p>none—Redistribute the PIM join states for the default master instance.</p> <p>instance <i>instance-name</i>—(Optional) Redistribute the join states 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>
Additional Information	The clear pim join-distribution command cannot be used to redistribute the PIM join states 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 neighbors on page 549• show pim join on page 527• join-load-balance on page 337
List of Sample Output	clear pim join-distribution on page 509
Output Fields	When you enter this command, you are provided no feedback on the status of your request. You can enter the show pim join command before and after distributing the join state to verify the operation.

Sample Output

clear pim join-distribution

```
user@host> clear pim join-distribution
```

clear pim register

List of Syntax	Syntax on page 510 Syntax (EX Series Switch and the QFX Series) on page 510 Syntax (PTX Series) on page 510
Syntax	<pre>clear pim register <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 register <inet inet6> <instance <i>instance-name</i>> <interface <i>interface-name</i>></pre>
Syntax (PTX Series)	<pre>clear pim register <inet inet6> <instance <i>instance-name</i>> <logical-system (all <i>logical-system-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 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. Command introduced in Junos OS Release 14.1X53-D20 for the OCX 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 563](#)

List of Sample Output [clear pim register on page 511](#)

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 512 Syntax (EX Series Switch and the QFX Series) on page 512
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	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. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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 563
List of Sample Output	clear pim statistics on page 513
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
...
```


request pim multicast-tunnel rebalance

List of Syntax	Syntax on page 515 Syntax (EX Series Switches) on page 515
Syntax	<pre>request pim multicast-tunnel rebalance <instance <i>instance-name</i>> <logical-system (all <i>logical-system-name</i>)></pre>
Syntax (EX Series Switches)	<pre>request pim multicast-tunnel rebalance <instance <i>instance-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 10.2.</p> <p>Command introduced in Junos OS Release 10.2 for EX Series switches.</p>
Description	<p>Rebalance the assignment of multicast tunnel encapsulation interfaces across available tunnel-capable PICs or across a configured list of tunnel-capable PICs. You can determine whether a rebalance is necessary by running the show pim interfaces instance <i>instance-name</i> command.</p>
Options	<p>none—Re-create and rebalance all tunnel interfaces for all routing instances.</p> <p>instance <i>instance-name</i>—Re-create and rebalance all tunnel interfaces for a specific 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	<p>maintenance</p>
Related Documentation	<ul style="list-style-type: none"> • show pim interfaces on page 524 • <i>Load Balancing Multicast Tunnel Interfaces Among Available PICs</i>
Output Fields	<p>This command produces no output. To verify the operation of the command, run the show pim interface instance <i>instance-name</i> before and after running the request pim multicast-tunnel rebalance command.</p>

show pim bidirectional df-election

Syntax	<pre>show pim bidirectional df-election <brief detail > <inet inet6> <instance <i>instance name</i>> <logical-system (all <i>logical-system-name</i>)> <rpa <i>address</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 12.1.</p> <p>Command introduced in Junos OS Release 13.3 for the PTX5000 router.</p>
Description	For bidirectional PIM, display the designated forwarder (DF) election results for each interface grouped by the rendezvous point addresses (RPAs).
Options	<p>none—Display standard information about all interfaces.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>inet inet6—(Optional) Display DF election results for IPv4 or IPv6 family addresses, respectively.</p> <p>instance <i>instance-name</i>—(Optional) Display DF election results for a specific 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>rpa <i>address</i>—(Optional) Display the DF election results for an RP address.</p>
Required Privilege Level	view
List of Sample Output	<p>show pim bidirectional df-election on page 517</p> <p>show pim bidirectional df-election brief on page 517</p>
Output Fields	Table 28 on page 516 describes the output fields for the show pim bidirectional df-election command. Output fields are listed in the approximate order in which they appear.

Table 28: show pim bidirectional df-election Output Fields

Field Name	Field Description	Level of Output
Family	IPv4 address family (INET) or IPv6 address family (INET6).	All levels
Instance	Name of the routing instance.	All levels
RPA	RP address.	All levels
Group ranges	Address ranges of the multicast groups mapped to this RP address.	All levels

Table 28: show pim bidirectional df-election Output Fields (*continued*)

Field Name	Field Description	Level of Output
Interfaces	Bidirectional PIM interfaces on this routing device. An interface can win the DF election (Win), lose the DF election (Lose), or be the RP link (RPL). The RP link is the interface directly connected to a subnet that contains a phantom RP address. A phantom RP address is an RP address that is not assigned to a routing device interface.	All levels brief displays the DF election winner only.
DF	IP address of the designated forwarder.	All levels

Sample Output

show pim bidirectional df-election

```

user@host> show pim bidirectional df-election
Instance: PIM.master Family: INET

RPA: 10.10.1.3
Group ranges: 224.1.3.0/24, 225.1.3.0/24
Interfaces:
    ge-0/0/1.0    (RPL)    DF: none
    lo0.0         (Win)     DF: 10.255.179.246
    xe-4/1/0.0    (Win)     DF: 10.10.2.1

RPA: 10.10.13.2
Group ranges: 224.1.1.0/24, 225.1.1.0/24
Interfaces:
    ge-0/0/1.0    (Lose)    DF: 10.10.1.2
    lo0.0         (Win)     DF: 10.255.179.246
    xe-4/1/0.0    (Lose)    DF: 10.10.2.2

Instance: PIM.master Family: INET6

RPA: fec0::10:10:1:3
Group ranges: ff00::/8
Interfaces:
    ge-0/0/1.0    (Lose)    DF: fe80::b2c6:9aff:fe95:86fa
    lo0.0         (Win)     DF: fe80::2a0:a50f:fc64:e661
    xe-4/1/0.0    (Win)     DF: fe80::226:88ff:fec5:3c37

RPA: fec0::10:10:13:2
Group ranges: ff00::/8
Interfaces:
    ge-0/0/1.0    (Lose)    DF: fe80::b2c6:9aff:fe95:86fa
    lo0.0         (Win)     DF: fe80::2a0:a50f:fc64:e661
    xe-4/1/0.0    (Win)     DF: fe80::226:88ff:fec5:3c37

```

show pim bidirectional df-election brief

```

user@host> show pim bidirectional df-election brief
Instance: PIM.master Family: INET

RPA: 10.10.1.3
Group ranges: 224.1.3.0/24, 225.1.3.0/24
Interfaces:
    lo0.0         (Win)     DF: 10.255.179.246
    xe-4/1/0.0    (Win)     DF: 10.10.2.1

```

```

RPA: 10.10.13.2
Group ranges: 224.1.1.0/24, 225.1.1.0/24
Interfaces:
    lo0.0          (Win)      DF: 10.255.179.246

Instance: PIM.master Family: INET6

RPA: fec0::10:10:1:3
Group ranges: ff00::/8
Interfaces:
    lo0.0          (Win)      DF: fe80::2a0:a50f:fc64:e661
    xe-4/1/0.0     (Win)      DF: fe80::226:88ff:fec5:3c37

RPA: fec0::10:10:13:2
Group ranges: ff00::/8
Interfaces:
    lo0.0          (Win)      DF: fe80::2a0:a50f:fc64:e661
    xe-4/1/0.0     (Win)      DF: fe80::226:88ff:fec5:3c37

```


show pim bidirectional df-election interface

Syntax	show pim bidirectional df-election interface <inet inet6> <instance <i>instance name</i> > < <i>interface-name</i> > <logical-system (all <i>logical-system-name</i>)>
Release Information	Command introduced in Junos OS Release 12.1. Command introduced in Junos OS Release 13.3 for the PTX5000 router.
Description	For bidirectional PIM, display the default and the configured designated forwarder (DF) election parameters for each interface.
Options	<p>none—Display standard information about all interfaces.</p> <p>inet inet6—(Optional) Display DF election parameters for IPv4 or IPv6 family addresses, respectively.</p> <p>instance <i>instance-name</i>—(Optional) Display DF election parameters for a specific routing instance.</p> <p><i>interface-name</i>—(Optional) Display DF election parameters 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>
Required Privilege Level	view
List of Sample Output	show pim bidirectional df-election interface on page 520
Output Fields	Table 29 on page 519 describes the output fields for the show pim bidirectional df-election interface command. Output fields are listed in the approximate order in which they appear.

Table 29: show pim bidirectional df-election interface Output Fields

Field Name	Field Description
Instance	Name of the routing instance.
Family	IPv4 address family (INET) or IPv6 address family (INET6).
Interface	Name of the bidirectional PIM interface.
Robustnes Count	Minimum number of DF election messages that must fail to be received for DF election to fail.
Offer Period	Interval between repeated DF election messages.
Backoff Period	Period that the acting DF waits between receiving a better DF Offer and sending the Pass message to transfer DF responsibility.

Table 29: show pim bidirectional df-election interface Output Fields (*continued*)

Field Name	Field Description
RPA	RP address.
State	For each RP address, state of each interface with respect to the DF election: Offer (when the election is in progress), Win , or Lose .
DF	IP address of the designated forwarder.

Sample Output

show pim bidirectional df-election interface

```

user@host> show pim bidirectional df-election interface
Instance: PIM.master Family: INET

Interface: ge-0/0/1.0
  Robustness Count: 3
  Offer Period: 100 ms
  Backoff Period: 1000 ms

  RPA                               State  DF
  10.10.1.3                         Offer  none
  10.10.13.2                       Lose   10.10.1.2

Interface: lo0.0
  Robustness Count: 3
  Offer Period: 100 ms
  Backoff Period: 1000 ms

  RPA                               State  DF
  10.10.1.3                         Win    10.255.179.246
  10.10.13.2                       Win    10.255.179.246

Interface: xe-4/1/0.0
  Robustness Count: 3
  Offer Period: 100 ms
  Backoff Period: 1000 ms

  RPA                               State  DF
  10.10.1.3                         Win    10.10.2.1
  10.10.13.2                       Lose   10.10.2.2

Instance: PIM.master Family: INET6

Interface: ge-0/0/1.0
  Robustness Count: 3
  Offer Period: 100 ms
  Backoff Period: 1000 ms

  RPA                               State  DF
  fec0::10:10:1:3                   Lose   fe80::b2c6:9aff:fe95:86fa
  fec0::10:10:13:2                  Lose   fe80::b2c6:9aff:fe95:86fa

Interface: lo0.0

```

Robustness Count: 3
Offer Period: 100 ms
Backoff Period: 1000 ms

RPA	State	DF
fec0::10:10:1:3	Win	fe80::2a0:a50f:fc64:e661
fec0::10:10:13:2	Win	fe80::2a0:a50f:fc64:e661

Interface: xe-4/1/0.0
Robustness Count: 3
Offer Period: 100 ms
Backoff Period: 1000 ms

RPA	State	DF
fec0::10:10:1:3	Win	fe80::226:88ff:fec5:3c37
fec0::10:10:13:2	Win	fe80::226:88ff:fec5:3c37

show pim bootstrap

List of Syntax	Syntax on page 522 Syntax (EX Series Switch and the QFX Series) on page 522
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> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX 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 523 show pim bootstrap instance on page 523
Output Fields	<p>Table 30 on page 522 describes the output fields for the show pim bootstrap command. Output fields are listed in the approximate order in which they appear.</p>

Table 30: 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.

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

Field Name	Field Description
Pri	Local routing device address priority to be elected as the bootstrap router.
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 524](#)
[Syntax \(EX Series Switch and the QFX Series\) on page 524](#)

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

Syntax (EX Series Switch and the QFX Series) show pim interfaces
 <inet | inet6>
 <instance (*instance-name* | all)>

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 the interfaces on which Protocol Independent Multicast (PIM) is configured.

Options **none**—Display interface information for all family addresses for the main instance.

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

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

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 525](#)

Output Fields [Table 31 on page 524](#) describes the output fields for the **show pim interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 31: show pim interfaces Output Fields

Field Name	Field Description
Instance	Name of the routing instance.
Name	Interface name.

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

Field Name	Field Description
State	State of the interface. The state also is displayed in the show interfaces command.
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. <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 527](#)
[Syntax \(EX Series Switch and the QFX Series\) on page 527](#)

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 506](#)
- *Example: Configuring Multicast-Only Fast Reroute in a PIM Domain*
- *Example: Configuring Bidirectional PIM*
- *Example: Configuring PIM State Limits*

List of Sample Output

[show pim join summary on page 533](#)
[show pim join \(PIM Sparse Mode\) on page 533](#)
[show pim join \(Bidirectional PIM\) on page 533](#)
[show pim join inet6 on page 534](#)
[show pim join inet6 star-g on page 534](#)
[show pim join instance <instance-name> on page 534](#)
[show pim join detail on page 535](#)
[show pim join extensive \(PIM Sparse Mode\) on page 535](#)
[show pim join extensive \(Bidirectional PIM\) on page 536](#)
[show pim join extensive \(Bidirectional PIM with a Directly Connected Phantom RP\) on page 537](#)
[show pim join instance <instance-name> extensive on page 538](#)
[show pim join extensive \(Ingress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs\) on page 538](#)
[show pim join extensive \(Egress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs\) on page 539](#)
[show pim join summary on page 541](#)
[show pim join \(PIM Sparse Mode\) on page 541](#)
[show pim join \(Bidirectional PIM\) on page 542](#)
[show pim join inet6 on page 542](#)
[show pim join inet6 star-g on page 543](#)
[show pim join instance <instance-name> on page 543](#)
[show pim join detail on page 543](#)

[show pim join extensive \(PIM Sparse Mode\) on page 544](#)
[show pim join extensive \(Bidirectional PIM\) on page 545](#)
[show pim join extensive \(Bidirectional PIM with a Directly Connected Phantom RP\) on page 546](#)
[show pim join instance <instance-name> extensive on page 546](#)
[show pim join extensive \(Ingress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs\) on page 547](#)
[show pim join extensive \(Multipoint LDP with Multicast-Only Fast Reroute\) on page 548](#)

Output Fields [Table 32 on page 529](#) describes the output fields for the **show pim join** command. Output fields are listed in the approximate order in which they appear.

Table 32: 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

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

Field Name	Field Description	Level of Output
Flags	<p>PIM flags:</p> <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
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
Active upstream interface	<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

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

Field Name	Field Description	Level of Output
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
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

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

Field Name	Field Description	Level of Output
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
Number of downstream interfaces	Total number of outgoing interfaces for each (S,G) entry.	extensive
Assert Timeout	Length of time between assert cycles on the downstream interface. Not displayed if the assert timer is null.	extensive
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 routing device 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 549 Syntax (EX Series Switch and the QFX Series) on page 549
Syntax	<pre>show pim neighbors <brief detail> <inet inet6> <instance (<i>instance-name</i> all)> <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> all)></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>Support for the instance all option 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) 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 551 show pim neighbors brief on page 551 show pim neighbors instance on page 551 show pim neighbors detail on page 551 show pim neighbors detail (With BFD) on page 552
Output Fields	<p>Table 33 on page 550 describes the output fields for the show pim neighbors command. Output fields are listed in the approximate order in which they appear.</p>

Table 33: 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 33: 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 551](#).

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, tsf
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 553 Syntax (EX Series Switch and the QFX Series) on page 553
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 556 show pim rps brief on page 556

[show pim rps <group-address> on page 556](#)
[show pim rps <group-address> on page 556](#)
[show pim rps <group-address> \(Bidirectional PIM\) on page 557](#)
[show pim rps <group-address> \(PIM Dense Mode\) on page 557](#)
[show pim rps <group-address> \(SSM Range Without asm-override-ssm Configured\) on page 557](#)
[show pim rps <group-address> \(SSM Range With asm-override-ssm Configured and a Sparse-Mode RP\) on page 557](#)
[show pim rps <group-address> \(SSM Range With asm-override-ssm Configured and a Bidirectional RP\) on page 557](#)
[show pim rps instance on page 557](#)
[show pim rps extensive \(PIM Sparse Mode\) on page 557](#)
[show pim rps extensive \(Bidirectional PIM\) on page 558](#)
[show pim rps extensive \(PIM Anycast RP in Use\) on page 558](#)

Output Fields [Table 34 on page 554](#) describes the output fields for the **show pim rps** command. Output fields are listed in the approximate order in which they appear.

Table 34: 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 34: 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 34: 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
100.100.100.100 auto-rp   sparse   150     146      0 235.0.0.0/8
                                     235.100.100.0/24
200.200.200.200 auto-rp   sparse   150     146      0 224.0.0.0/4

address-family INET6

```

show pim rps brief

The output for the **show pim rps brief** command is identical to that for the **show pim rps** command. For sample output, see [show pim rps on page 556](#).

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>

```

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 560 Syntax (EX Series Switch and the QFX Series) on page 560
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	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. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
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 561 show pim source brief on page 561 show pim source detail on page 561 show pim source (Egress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 562

Output Fields [Table 35 on page 561](#) describes the output fields for the **show pim source** command. Output fields are listed in the approximate order in which they appear.

Table 35: 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 Protocol	Protocol toward the source address.
Upstream interface	RPF interface toward the source address. A pseudo multipoint LDP (M-LDP) interface appears on egress nodes in M-LDP point-to-multipoint LSPs with inband signaling.
Upstream Neighbor	Address of the RPF neighbor used to reach the source address. The multipoint LDP (M-LDP) root appears on egress nodes in M-LDP point-to-multipoint LSPs with inband signaling.

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 561](#).

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 source (Egress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

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

Source 1.1.1.1
Prefix 1.1.1.1/32
Upstream interface Local
Upstream neighbor Local

Source 1.2.7.7
Prefix 1.2.7.0/24
Upstream protocol MLDP
Upstream interface Pseudo MLDP
Upstream neighbor MLDP LSP root <1.1.1.2>

Source 192.168.219.11
Prefix 192.168.219.0/28
Upstream protocol MLDP
Upstream interface Pseudo MLDP
Upstream neighbor MLDP LSP root <1.1.1.2>

Instance: PIM.master Family: INET6

Source abcd::1:2:7:7
Prefix abcd::1:2:7:0/120
Upstream protocol MLDP
Upstream interface Pseudo MLDP
Upstream neighbor MLDP LSP root <1.1.1.2>
```

show pim statistics

List of Syntax	Syntax on page 563 Syntax (EX Series Switch and the QFX Series) on page 563
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> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</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 512
List of Sample Output	show pim statistics on page 570 show pim statistics inet interface <interface-name> on page 572 show pim statistics inet6 interface <interface-name> on page 572 show pim statistics instance <instance-name> on page 573 show pim statistics interface <interface-name> on page 574
Output Fields	<p>Table 36 on page 564 describes the output fields for the show pim statistics command. Output fields are listed in the approximate order in which they appear.</p>

Table 36: 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.
V2 State Refresh	<p>PIM version 2 control messages related to PIM dense mode (PIM-DM) state refresh.</p> <p>State refresh is an extension to PIM-DM. It not supported in Junos OS.</p>

Table 36: show pim statistics Output Fields (*continued*)

Field Name	Field Description
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.
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.

Table 36: show pim statistics Output Fields (*continued*)

Field Name	Field Description
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 routing device 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 routing device 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 routing device has no state.
Rx Join/Prune on upstream if	Number of join and prune messages received on the interface used to reach the upstream routing device, toward the RP.
Rx Join/Prune for invalid group	Number of join or prune messages received for invalid multicast group addresses.
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.

Table 36: show pim statistics Output Fields (*continued*)

Field Name	Field Description
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 routing device, 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 routing device has no state for the data type.
Rx RP no state	Number of PIM control packets received for which the routing device 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 routing device does not have an encapsulation interface.
No route upstream	Number of PIM control packets received when the routing device does not have a unicast route to the the interface used to reach the upstream routing device, 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 routing device has an RP mismatch.
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 routing device has an unknown RPF neighbor for the source.

Table 36: show pim statistics Output Fields (*continued*)

Field Name	Field Description
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 routing device:</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.
Rx Bidir Join/Prune on non-DF if	Error counter for join and prune messages received on non-designated forwarder interfaces.
V4 (S,G) Maximum	Maximum number of (S,G) IPv4 multicast routes accepted for the VPN routing and forwarding (VRF) routing instance. If this number is met, additional (S,G) entries are not accepted.

Table 36: show pim statistics Output Fields (*continued*)

Field Name	Field Description
V4 (S,G) Accepted	Number of accepted (S,G) IPv4 multicast routes.
V4 (S,G) Threshold	Threshold at which a warning message is logged (percentage of the maximum number of (S,G) IPv4 multicast routes accepted by the device).
V4 (S,G) Log Interval	Time (in seconds) between consecutive log messages.
V6 (S,G) Maximum	Maximum number of (S,G) IPv6 multicast routes accepted for the VPN routing and forwarding (VRF) routing instance. If this number is met, additional (S,G) entries are not accepted.
V6 (S,G) Accepted	Number of accepted (S,G) IPv6 multicast routes.
V6 (S,G) Threshold	Threshold at which a warning message is logged (percentage of the maximum number of (S,G) IPv6 multicast routes accepted by the device).
V6 (S,G) Log Interval	Time (in seconds) between consecutive log messages.
V4 (grp-prefix, RP) Maximum	Maximum number of group-to-rendezvous point (RP) IPv4 multicast mappings accepted for the VRF routing instance. If this number is met, additional mappings are not accepted.
V4 (grp-prefix, RP) Accepted	Number of accepted group-to-RP IPv4 multicast mappings.
V4 (grp-prefix, RP) Threshold	Threshold at which a warning message is logged (percentage of the maximum number of group-to-RP IPv4 multicast mappings accepted by the device).
V4 (grp-prefix, RP) Log Interval	Time (in seconds) between consecutive log messages.
V6 (grp-prefix, RP) Maximum	Maximum number of group-to RP IPv6 multicast mappings accepted for the VRF routing instance. If this number is met, additional mappings are not accepted.
V6 (grp-prefix, RP) Accepted	Number of accepted group-to-RP IPv6 multicast mappings.
V6 (grp-prefix, RP) Threshold	Threshold at which a warning message is logged (percentage of the maximum number of group-to-RP IPv6 multicast mappings accepted by the device).
V6 (grp-prefix, RP) Log Interval	Time (in seconds) between consecutive log messages.

Table 36: show pim statistics Output Fields (*continued*)

Field Name	Field Description
V4 Register Maximum	Maximum number of IPv4 PIM registers accepted for the VRF routing instance. If this number is met, additional PIM registers are not accepted. You configure the register limits on the RP.
V4 Register Accepted	Number of accepted IPv4 PIM registers.
V4 Register Threshold	Threshold at which a warning message is logged (percentage of the maximum number of IPv4 PIM registers accepted by the device).
V4 Register Log Interval	Time (in seconds) between consecutive log messages.
V6 Register Maximum	Maximum number of IPv6 PIM registers accepted for the VRF routing instance. If this number is met, additional PIM registers are not accepted. You configure the register limits on the RP.
V6 Register Accepted	Number of accepted IPv6 PIM registers.
V6 Register Threshold	Threshold at which a warning message is logged (percentage of the maximum number of IPv6 PIM registers accepted by the device).
V6 Register Log Interval	Time (in seconds) between consecutive log messages.
(*G) Join drop due to SSM range check	PIM join messages that are dropped because the multicast addresses are outside of the SSM address range of 232.0.0.0 through 232.255.255.255. You can extend the accepted SSM address range by configuring the ssm-groups statement.

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		
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
ipv4 BSR pkt drop due to excessive rate	0
ipv6 BSR pkt drop due to excessive rate	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
(*,G) Join drop due to SSM range check 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

show pim statistics instance <instance-name>

```

user@host> show pim statistics instance VPN-A
PIM Message type      Received      Sent  Rx errors
V2 Hello               31           37      0
V2 Register            0            0      0
V2 Register Stop       0            0      0
V2 Join Prune          0           16      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        0
Rx Join/Prune messages dropped         0
Rx sparse join for dense group         0
Rx Graft/Graft Ack no state            0
Rx Graft on upstream if                0
Rx CRP not BSR                        0
Rx BSR when BSR                       0
Rx BSR not RPF if                     0
Rx unknown hello opt                  0
Rx data no state                      0

```

Rx RP no state	0
Rx aggregate	0
Rx malformed packet	0
Rx illegal TTL	0
Rx illegal destination address	0
No RP	0
No register encap if	0
No route upstream	28
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
V4 (S,G) Maximum	10
V4 (S,G) Accepted	9
V4 (S,G) Threshold	80
V4 (S,G) Log Interval	80
V6 (S,G) Maximum	8
V6 (S,G) Accepted	8
V6 (S,G) Threshold	50
V6 (S,G) Log Interval	100
V4 (grp-prefix, RP) Maximum	100
V4 (grp-prefix, RP) Accepted	5
V4 (grp-prefix, RP) Threshold	80
V4 (grp-prefix, RP) Log Interval	10
V6 (grp-prefix, RP) Maximum	20
V6 (grp-prefix, RP) Accepted	0
V6 (grp-prefix, RP) Threshold	90
V6 (grp-prefix, RP) Log Interval	20
V4 Register Maximum	100
V4 Register Accepted	10
V4 Register Threshold	80
V4 Register Log Interval	10
V6 Register Maximum	20
V6 Register Accepted	0
V6 Register Threshold	90
V6 Register Log Interval	20
(*,G) Join drop due to SSM range check	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

