

HP 5500 EI & 5500 SI Switch Series

IP Multicast

Configuration Guide

Part number: 5998-1712

Software version: Release 2220

Document version: 6W100-20130810



Legal and notice information

© Copyright 2013 Hewlett-Packard Development Company, L.P.

No part of this documentation may be reproduced or transmitted in any form or by any means without prior written consent of Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Contents

Multicast overview	1
Introduction to multicast	1
Information transmission techniques	1
Multicast features	4
Common notations in multicast	5
Multicast advantages and applications	5
Multicast models	6
Multicast architecture	7
Multicast addresses	7
Multicast protocols	11
Multicast packet forwarding mechanism	13
Multicast support for VPNs	13
Introduction to VPN instances	14
Multicast application in VPNs	14
Configuring IGMP snooping	16
Overview	16
Basic concepts in IGMP snooping	16
How IGMP snooping works	18
IGMP snooping proxying	20
Protocols and standards	21
IGMP snooping configuration task list	21
Configuring basic IGMP snooping functions	22
Enabling IGMP snooping	23
Specifying the version of IGMP snooping	23
Configuring static multicast MAC address entries	24
Configuring IGMP snooping port functions	24
Setting aging timers for dynamic ports	25
Configuring static ports	25
Configuring a port as a simulated member host	26
Enabling IGMP snooping fast-leave processing	27
Disabling a port from becoming a dynamic router port	28
Configuring IGMP snooping querier	29
Enabling IGMP snooping querier	29
Configuring parameters for IGMP queries and responses	29
Configuring the source IP addresses for IGMP queries	30
Configuring IGMP snooping proxying	31
Enabling IGMP snooping proxying	31
Configuring a source IP address for the IGMP messages sent by the proxy	31

Configuring an IGMP snooping policy.....	32
Configuring a multicast group filter.....	32
Configuring multicast source port filtering.....	33
Enabling dropping unknown multicast data.....	34
Configuring IGMP report suppression.....	34
Setting the maximum number of multicast groups that a port can join.....	35
Enabling multicast group replacement.....	36
Setting the 802.1p precedence for IGMP messages.....	37
Configuring a multicast user control policy.....	37
Enabling the IGMP snooping host tracking function.....	38
Setting the DSCP value for IGMP messages.....	39
Displaying and maintaining IGMP snooping.....	39
IGMP snooping configuration examples.....	40
Group policy and simulated joining configuration example.....	40
Static port configuration example.....	42
IGMP snooping querier configuration example.....	46
IGMP snooping proxying configuration example.....	48
Multicast source and user control policy configuration example.....	50
Troubleshooting IGMP snooping.....	55
Layer 2 multicast forwarding cannot function.....	55
Configured multicast group policy fails to take effect.....	56
Appendix.....	56
Processing of multicast protocol messages.....	56
Configuring PIM snooping.....	58
Overview.....	58
Configuring PIM snooping.....	59
Displaying and maintaining PIM snooping.....	60
PIM snooping configuration example.....	60
Troubleshooting PIM snooping.....	63
PIM snooping does not work.....	63
Some downstream PIM-capable routers cannot receive multicast data.....	63
Configuring multicast VLANs.....	65
Overview.....	65
Multicast VLAN configuration task list.....	67
Configuring a sub-VLAN-based multicast VLAN.....	67
Configuration guidelines.....	67
Configuration procedure.....	67
Configuring a port-based multicast VLAN.....	68
Configuration prerequisites.....	68
Configuring user port attributes.....	68
Configuring multicast VLAN ports.....	69
Displaying and maintaining multicast VLAN.....	70
Multicast VLAN configuration examples.....	70

Sub-VLAN-based multicast VLAN configuration example	70
Port-based multicast VLAN configuration example	74
Configuring multicast routing and forwarding (available only on the HP 5500 EI)	78
Overview	78
RPF check mechanism	78
Static multicast routes	81
Multicast forwarding across unicast subnets	83
Multicast traceroute	84
Configuration task list	85
Enabling IP multicast routing	85
Configuring multicast routing and forwarding	86
Configuring static multicast routes	86
Configuring a multicast routing policy	87
Configuring a multicast forwarding range	87
Configuring the multicast forwarding table size	88
Tracing a multicast path	89
Displaying and maintaining multicast routing and forwarding	89
Configuration examples	91
Changing an RPF route	91
Creating an RPF route	93
Multicast forwarding over a tunnel	95
Troubleshooting multicast routing and forwarding	99
Static multicast route failure	99
Multicast data fails to reach receivers	100
Configuring IGMP (available only on the HP 5500 EI)	101
Overview	101
IGMP versions	101
Introduction to IGMPv1	101
Enhancements in IGMPv2	103
Enhancements in IGMPv3	104
IGMP SSM mapping	105
IGMP proxying	106
IGMP support for VPNs	108
Protocols and standards	108
IGMP configuration task list	108
Configuring basic IGMP functions	109
Enabling IGMP	109
Configuring IGMP versions	110
Configuring static joining	110
Configuring a multicast group filter	111
Setting the maximum number of multicast groups that an interface can join	111
Adjusting IGMP performance	112
Configuration prerequisites	112

Configuring Router-Alert option handling methods.....	112
Configuring IGMP query and response parameters.....	113
Configuring IGMP fast-leave processing	116
Enabling the IGMP host tracking function	117
Setting the DSCP value for IGMP messages.....	117
Configuring IGMP SSM mapping	118
Enabling SSM mapping.....	118
Configuring SSM mappings.....	118
Configuring IGMP proxying	119
Enabling IGMP proxying.....	119
Configuring multicast forwarding on a downstream interface.....	120
Displaying and maintaining IGMP.....	120
IGMP configuration examples	122
Basic IGMP functions configuration example.....	122
SSM mapping configuration example	124
IGMP proxying configuration example.....	127
Troubleshooting IGMP.....	129
No membership information on the receiver-side router.....	129
Inconsistent memberships on routers on the same subnet.....	130
Configuring PIM (available only on the HP 5500 EI)	131
PIM overview	131
PIM-DM overview	131
PIM-SM overview.....	134
BIDIR-PIM overview.....	140
Administrative scoping overview.....	144
PIM-SSM overview.....	146
Relationships among PIM protocols	148
PIM support for VPNs.....	148
Protocols and standards	148
Configuring PIM-DM	149
PIM-DM configuration task list.....	149
Configuration prerequisites	149
Enabling PIM-DM.....	149
Enabling state-refresh capability.....	150
Configuring state-refresh parameters	151
Configuring PIM-DM graft retry period.....	151
Configuring PIM-SM.....	152
PIM-SM configuration task list.....	152
Configuration prerequisites	152
Enabling PIM-SM	153
Configuring an RP	154
Configuring a BSR.....	156
Configuring administrative scoping	160

Configuring multicast source registration.....	162
Disabling the switchover to SPT.....	163
Configuring BIDIR-PIM.....	164
BIDIR-PIM configuration task list.....	164
Configuration prerequisites.....	164
Enabling PIM-SM.....	165
Enabling BIDIR-PIM.....	166
Configuring an RP.....	166
Configuring a BSR.....	168
Configuring administrative scoping.....	172
Configuring PIM-SSM.....	174
PIM-SSM configuration task list.....	174
Configuration prerequisites.....	175
Enabling PIM-SM.....	175
Configuring the SSM group range.....	176
Configuring PIM common features.....	176
PIM common feature configuration task list.....	176
Configuration prerequisites.....	177
Configuring a multicast data filter.....	177
Configuring a hello message filter.....	178
Configuring PIM hello options.....	178
Configuring the prune delay.....	180
Configuring PIM common timers.....	181
Configuring join/prune message sizes.....	182
Configuring PIM to work with BFD.....	182
Setting the DSCP value for PIM messages.....	183
Displaying and maintaining PIM.....	183
PIM configuration examples.....	185
PIM-DM configuration example.....	185
PIM-SM non-scoped zone configuration example.....	188
PIM-SM admin-scope zone configuration example.....	194
BIDIR-PIM configuration example.....	200
PIM-SSM configuration example.....	205
Troubleshooting PIM.....	208
A multicast distribution tree cannot be built correctly.....	208
Multicast data abnormally terminated on an intermediate router.....	209
RPs cannot join SPT in PIM-SM.....	209
RPT establishment failure or source registration failure in PIM-SM.....	210
Configuring MSDP (available only on the HP 5500 EI).....	211
Overview.....	211
How MSDP works.....	212
MSDP support for VPNs.....	217
Protocols and standards.....	217

MSDP configuration task list	217
Configuring basic MSDP functions.....	218
Configuration prerequisites	218
Enabling MSDP.....	218
Creating an MSDP peer connection.....	219
Configuring a static RPF peer	219
Configuring an MSDP peer connection.....	220
Configuring MSDP peer description.....	220
Configuring an MSDP mesh group	220
Configuring MSDP peer connection control.....	221
Configuring SA messages related parameters	222
Configuring SA message content	222
Configuring SA request messages.....	223
Configuring SA message filtering rules.....	224
Configuring the SA cache mechanism.....	224
Displaying and maintaining MSDP.....	225
MSDP configuration examples.....	226
PIM-SM Inter-domain multicast configuration	226
Inter-AS multicast configuration by leveraging static RPF peers	231
Anycast RP configuration.....	235
SA message filtering configuration.....	239
Troubleshooting MSDP	243
MSDP peers stay in down state	243
No SA entries in the switch's SA cache.....	243
Inter-RP communication faults in Anycast RP application	244
Configuring MBGP (available only on the HP 5500 EI).....	245
MBGP overview.....	245
Protocols and standards	245
MBGP configuration task list.....	245
Configuring basic MBGP functions.....	246
Controlling route advertisement and reception.....	247
Configuring MBGP route redistribution.....	247
Configuring default route redistribution into MBGP	247
Configuring MBGP route summarization.....	248
Advertising a default route to an IPv4 MBGP peer or peer group	249
Configuring outbound MBGP route filtering.....	249
Configuring inbound MBGP route filtering.....	250
Configuring MBGP route dampening	251
Configuring MBGP route attributes	252
Configuring MBGP route preferences	252
Configuring the default local preference	252
Configuring the MED attribute	253
Configuring the NEXT_HOP attribute.....	253

Configuring the AS_PATH attributes	254
Tuning and optimizing MBGP networks	254
Configuring MBGP soft reset	254
Enabling the MBGP ORF capability	256
Configuring the maximum number of MBGP routes for load balancing	257
Configuring a large scale MBGP network	257
Configuring IPv4 MBGP peer groups	257
Configuring MBGP community	258
Configuring an MBGP route reflector	259
Displaying and maintaining MBGP	260
Displaying MBGP	260
Resetting MBGP connections	261
Clearing MBGP information	261
MBGP configuration example	261
Configuring MLD snooping	266
Overview	266
Basic concepts in MLD snooping	266
How MLD snooping works	268
MLD snooping proxying	269
Protocols and standards	271
MLD snooping configuration task list	271
Configuring basic MLD snooping functions	272
Enabling MLD snooping	272
Specifying the version of MLD snooping	273
Configuring IPv6 static multicast MAC address entries	273
Configuring MLD snooping port functions	274
Configuring aging timers for dynamic ports	274
Configuring static ports	275
Configuring a port as a simulated member host	276
Enabling fast-leave processing	277
Disabling a port from becoming a dynamic router port	278
Configuring MLD snooping querier	278
Enabling MLD snooping querier	279
Configuring parameters for MLD queries and responses	279
Configuring the source IPv6 addresses for MLD queries	280
Configuring MLD snooping proxying	281
Enabling MLD snooping proxying	281
Configuring the source IPv6 addresses for the MLD messages sent by the proxy	281
Configuring an MLD snooping policy	282
Configuring an IPv6 multicast group filter	282
Configuring IPv6 multicast source port filtering	283
Enabling dropping unknown IPv6 multicast data	284
Configuring MLD report suppression	284

Setting the maximum number of multicast groups that a port can join	285
Enabling IPv6 multicast group replacement	285
Setting the 802.1p precedence for MLD messages	286
Configuring an IPv6 multicast user control policy.....	287
Enabling the MLD snooping host tracking function	288
Setting the DSCP value for MLD messages.....	288
Displaying and maintaining MLD snooping.....	289
MLD snooping configuration examples	290
IPv6 group policy and simulated joining configuration example	290
Static port configuration example	292
MLD snooping querier configuration example.....	296
MLD snooping proxying configuration example.....	298
IPv6 multicast source and user control policy configuration example.....	300
Troubleshooting MLD snooping	305
Layer 2 multicast forwarding cannot function	305
Configured IPv6 multicast group policy fails to take effect.....	306
Appendix	306
Processing of IPv6 multicast protocol messages.....	306
Configuring IPv6 PIM snooping	308
Overview.....	308
Configuring IPv6 PIM snooping.....	309
Displaying and maintaining IPv6 PIM snooping	310
IPv6 PIM snooping configuration example.....	310
Troubleshooting IPv6 PIM snooping.....	313
IPv6 PIM snooping does not work.....	313
Some downstream IPv6 PIM-capable routers cannot receive multicast data	313
Configuring IPv6 multicast VLANs	315
Overview.....	315
IPv6 multicast VLAN configuration task list	317
Configuring a sub-VLAN-based IPv6 multicast VLAN	317
Configuration guidelines	317
Configuration procedure	318
Configuring a port-based IPv6 multicast VLAN	318
Configuration prerequisites	318
Configuring user port attributes	318
Configuring IPv6 multicast VLAN ports.....	319
Displaying and maintaining IPv6 multicast VLAN	320
IPv6 multicast VLAN configuration examples.....	320
Sub-VLAN-based multicast VLAN configuration example	320
Port-based multicast VLAN configuration example.....	325
Configuring IPv6 multicast routing and forwarding (available only on the HP 5500 EI).....	328
Overview.....	328

RPF check mechanism	328
RPF check implementation in IPv6 multicast	329
Configuration task list	331
Enabling IPv6 multicast routing	331
Configuring IPv6 multicast routing and forwarding	331
Configuring an IPv6 multicast routing policy	331
Configuring an IPv6 multicast forwarding range	332
Configuring the IPv6 multicast forwarding table size	332
Displaying and maintaining IPv6 multicast routing and forwarding	333
Troubleshooting IPv6 multicast policy configuration	335
Abnormal termination of IPv6 multicast data	335
Configuring MLD (available only on the HP 5500 EI)	336
Overview	336
MLD versions	336
How MLDv1 works	336
How MLDv2 works	338
MLD messages	340
MLD SSM mapping	342
MLD proxying	343
Protocols and standards	344
MLD configuration task list	344
Configuring basic MLD functions	345
Enabling MLD	345
Configuring the MLD version	346
Configuring static joining	346
Configuring an IPv6 multicast group filter	347
Setting the maximum number of IPv6 multicast groups that an interface can join	347
Adjusting MLD performance	348
Configuration prerequisites	348
Configuring Router-Alert option handling methods	348
Configuring MLD query and response parameters	349
Configuring MLD fast-leave processing	351
Enabling the MLD host tracking function	352
Setting the DSCP value for MLD messages	353
Configuring MLD SSM mapping	353
Configuration prerequisites	353
Enabling MLD SSM mapping	354
Configuring MLD SSM mappings	354
Configuring MLD proxying	354
Enabling MLD proxying	355
Configuring IPv6 multicast forwarding on a downstream interface	355
Displaying and maintaining MLD	356
MLD configuration examples	358

Basic MLD functions configuration example.....	358
MLD SSM mapping configuration example	360
MLD proxying configuration example.....	363
Troubleshooting MLD	364
No member information on the receiver-side router.....	364
Inconsistent memberships on routers on the same subnet.....	365
Configuring IPv6 PIM (available only on the HP 5500 EI).....	366
Overview.....	366
IPv6 PIM-DM overview.....	366
IPv6 PIM-SM overview	369
IPv6 BIDIR-PIM overview	376
IPv6 administrative scoping overview	380
IPv6 PIM-SSM overview	383
Relationship among IPv6 PIM protocols.....	384
Protocols and standards	385
Configuring IPv6 PIM-DM.....	385
IPv6 PIM-DM configuration task list.....	385
Configuration prerequisites	386
Enabling IPv6 PIM-DM	386
Enabling state-refresh capability.....	386
Configuring state refresh parameters.....	387
Configuring IPv6 PIM-DM graft retry period	388
Configuring IPv6 PIM-SM	388
IPv6 PIM-SM configuration task list.....	388
Configuration prerequisites	389
Enabling IPv6 PIM-SM.....	389
Configuring an RP	390
Configuring a BSR.....	392
Configuring IPv6 administrative scoping	396
Configuring IPv6 multicast source registration	397
Disabling the switchover to SPT	398
Configuring IPv6 BIDIR-PIM	399
IPv6 BIDIR-PIM configuration task list	399
Configuration prerequisites	399
Enabling IPv6 PIM-SM.....	400
Enabling IPv6 BIDIR-PIM	400
Configuring an RP	401
Configuring a BSR.....	403
Configuring IPv6 administrative scoping	407
Configuring IPv6 PIM-SSM	408
IPv6 PIM-SSM configuration task list	408
Configuration prerequisites	408
Enabling IPv6 PIM-SM.....	409

Configuring the IPv6 SSM group range	409
Configuring IPv6 PIM common features	410
IPv6 PIM common feature configuration task list	410
Configuration prerequisites	410
Configuring an IPv6 multicast data filter	411
Configuring a hello message filter	411
Configuring IPv6 PIM hello options	412
Configuring the prune delay	414
Configuring IPv6 PIM common timers	414
Configuring join/prune message sizes	415
Configuring IPv6 PIM to work with BFD	416
Setting the DSCP value for IPv6 PIM messages	417
Displaying and maintaining IPv6 PIM	417
IPv6 PIM configuration examples	418
IPv6 PIM-DM configuration example	418
IPv6 PIM-SM non-scoped zone configuration example	421
IPv6 PIM-SM admin-scope zone configuration example	426
IPv6 BIDIR-PIM configuration example	439
IPv6 PIM-SSM configuration example	444
Troubleshooting IPv6 PIM configuration	447
Failure to build a multicast distribution tree correctly	447
IPv6 multicast data abnormally terminated on an intermediate router	448
RPS cannot join SPT in IPv6 PIM-SM	448
RPT establishment failure or source registration failure in IPv6 PIM-SM	449
Configuring IPv6 MBGP (available only on the HP 5500 EI)	450
IPv6 MBGP overview	450
IPv6 MBGP configuration task list	450
Configuring basic IPv6 MBGP functions	451
Configuration prerequisites	451
Configuring an IPv6 MBGP peer	451
Configuring a preferred value for routes from a peer or a peer group	452
Controlling route distribution and reception	452
Configuration prerequisites	452
Injecting a local IPv6 MBGP route	452
Configuring IPv6 MBGP route redistribution	453
Configuring IPv6 MBGP route summarization	453
Advertising a default route to a peer or peer group	453
Configuring outbound IPv6 MBGP route filtering	454
Configuring inbound IPv6 MBGP route filtering	455
Configuring IPv6 MBGP route dampening	455
Configuring IPv6 MBGP route attributes	456
Configuration prerequisites	456
Configuring IPv6 MBGP route preferences	456

Configuring the default local preference	456
Configuring the MED attribute	457
Configuring the NEXT_HOP attribute	457
Configuring the AS_PATH attribute	458
Tuning and optimizing IPv6 MBGP networks	458
Configuration prerequisites	458
Configuring IPv6 MBGP soft reset	459
Enabling the IPv6 MBGP orf capability	460
Configuring the maximum number of equal-cost routes for load-balancing	461
Configuring a large scale IPv6 MBGP network	461
Configuring an IPv6 MBGP peer group	461
Configuring IPv6 MBGP community	462
Configuring an IPv6 MBGP route reflector	463
Displaying and maintaining IPv6 MBGP	463
Displaying IPv6 MBGP	463
Resetting IPv6 MBGP connections	465
Clearing IPv6 MBGP information	465
IPv6 MBGP configuration example	465
Support and other resources	469
Contacting HP	469
Subscription service	469
Related information	469
Documents	469
Websites	469
Conventions	470
Index	472

Multicast overview

Introduction to multicast

As a technique that coexists with unicast and broadcast, the multicast technique effectively addresses the issue of point-to-multipoint data transmission. By enabling high-efficiency point-to-multipoint data transmission over a network, multicast greatly saves network bandwidth and reduces network load.

By using multicast technology, a network operator can easily provide new value-added services, such as live webcasting, web TV, distance learning, telemedicine, web radio, real time video conferencing, and other bandwidth-critical and time-critical information services.

The term "router " in this document refers to both routers and Layer 3 switches.

Unless otherwise stated, the term "multicast" in this document refers to IP multicast.

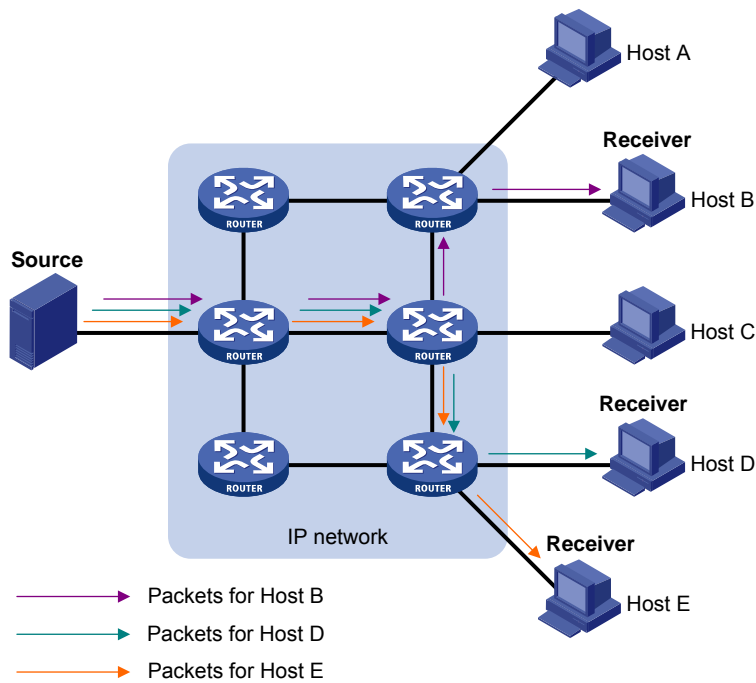
Information transmission techniques

The information transmission techniques include unicast, broadcast, and multicast.

Unicast

In unicast transmission, the information source must send a separate copy of information to each host that needs the information.

Figure 1 Unicast transmission



In [Figure 1](#), assume that Host B, Host D and Host E need the information. A separate transmission channel must be established from the information source to each of these hosts.

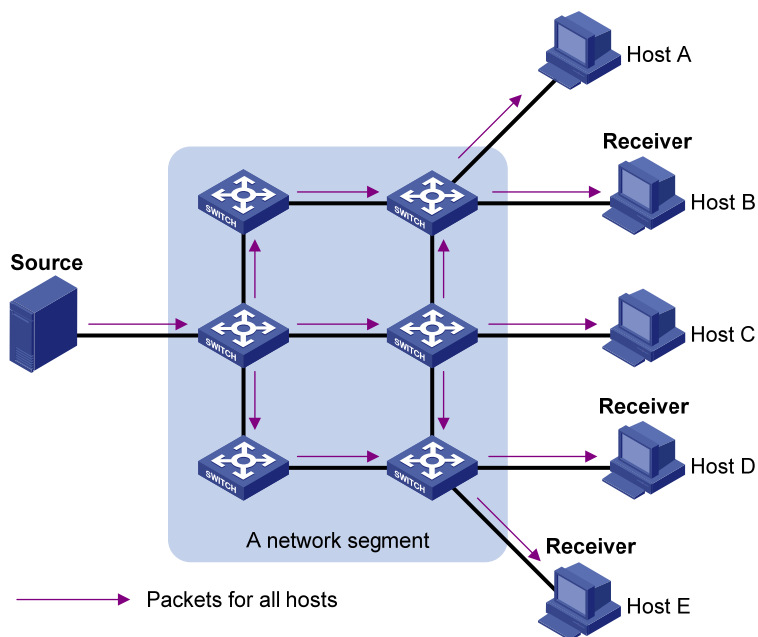
In unicast transmission, the traffic transmitted over the network is proportional to the number of hosts that need the information. If a large number of hosts need the information, the information source must send a separate copy of the same information to each of these hosts. Sending many copies can place a tremendous pressure on the information source and the network bandwidth.

Unicast is not suitable for batch transmission of information.

Broadcast

In broadcast transmission, the information source sends information to all hosts on the subnet, even if some hosts do not need the information.

Figure 2 Broadcast transmission



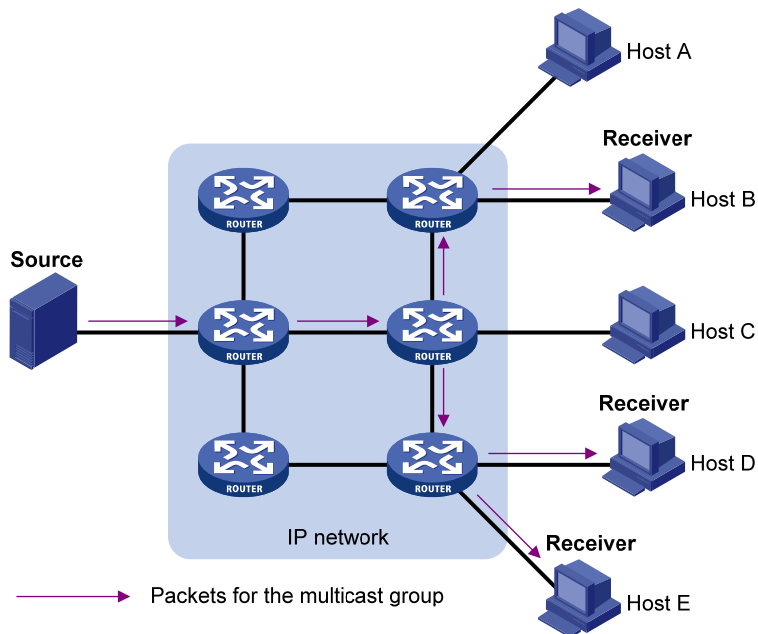
In Figure 2, assume that only Host B, Host D, and Host E need the information. If the information is broadcast to the subnet, Host A and Host C also receive it. In addition to information security issues, broadcasting to hosts that do not need the information also causes traffic flooding on the same subnet. Broadcast is disadvantageous in transmitting data to specific hosts. Moreover, broadcast transmission is a significant waste of network resources.

Multicast

Unicast and broadcast techniques cannot provide point-to-multipoint data transmissions with the minimum network consumption.

Multicast transmission can solve this problem. When some hosts on the network need multicast information, the information sender, or multicast source, sends only one copy of the information. Multicast distribution trees are built through multicast routing protocols, and the packets are replicated only on nodes where the trees branch.

Figure 3 Multicast transmission



The multicast source sends only one copy of the information to a multicast group. Host B, Host D and Host E, which are receivers of the information, must join the multicast group. The routers on the network duplicate and forward the information based on the distribution of the group members. Finally, the information is correctly delivered to Host B, Host D, and Host E.

To summarize, multicast has the following advantages:

- **Advantages over unicast**—Because multicast traffic flows to the farthest-possible node from the source before it is replicated and distributed, an increase in the number of hosts does not increase the load of the source or remarkably add to the usage of network resources.
- **Advantages over broadcast**—Because multicast data is sent only to the receivers that need it, multicast uses network bandwidth reasonably and enhances network security. In addition, data broadcast is confined to the same subnet, but multicast is not.

Multicast features

- A multicast group is a multicast receiver set identified by an IP multicast address. Hosts join a multicast group to become members of the multicast group before they can receive the multicast data addressed to that multicast group. Typically, a multicast source does not need to join a multicast group.
- An information sender is called a "multicast source". A multicast source can send data to multiple multicast groups at the same time, and multiple multicast sources can send data to the same multicast group at the same time.

- All hosts that have joined a multicast group become members of the multicast group. The group memberships are dynamic. Hosts can join or leave multicast groups at any time. Multicast groups are not subject to geographic restrictions.
- Routers or Layer 3 switches that support Layer 3 multicast are called "multicast routers" or "Layer 3 multicast devices". In addition to providing the multicast routing function, a multicast router can also manage multicast group memberships on stub subnets with attached group members. A multicast router itself can be a multicast group member.

For a better understanding of the multicast concept, you can compare multicast transmission to the transmission of TV programs.

Table 1 Comparing TV program transmission and multicast transmission

TV transmission	Multicast transmission
A TV station transmits a TV program through a channel.	A multicast source sends multicast data to a multicast group.
A user tunes the TV set to the channel.	A receiver joins the multicast group.
The user starts to watch the TV program transmitted by the TV station via the channel.	The receiver starts to receive the multicast data that the source is sending to the multicast group.
The user turns off the TV set or tunes to another channel.	The receiver leaves the multicast group or joins another group.

Common notations in multicast

The following notations are commonly used in multicast transmission:

- **(*, G)**—Indicates a rendezvous point tree (RPT), or a multicast packet that any multicast source sends to multicast group G. Here, the asterisk represents any multicast source, and "G" represents a specific multicast group.
- **(S, G)**—Indicates a shortest path tree (SPT), or a multicast packet that multicast source S sends to multicast group G. Here, "S" represents a specific multicast source, and "G" represents a specific multicast group.

For more information about the concepts RPT and SPT, see "[Configuring PIM \(available only on the HP 5500 EI\)](#)" and "[Configuring IPv6 PIM \(available only on the HP 5500 EI\)](#)."

Multicast advantages and applications

Multicast advantages

Advantages of the multicast technique include the following:

- **Enhanced efficiency**—Reduces the processor load of information source servers and network devices.
- **Optimal performance**—Reduces redundant traffic.

- **Distributed application**—Enables point-to-multipoint applications at the price of minimum network resources.

Multicast applications

The scenarios in which the multicast technique can be effectively applied are:

- Multimedia and streaming applications, such as web TV, web radio, and real time video/audio conferencing
- Communication for training and cooperative operations, such as distance learning and telemedicine
- Data warehouse and financial applications (stock quotes)
- Any other point-to-multipoint application for data distribution

Multicast models

Based on how the receivers treat the multicast sources, the multicast models include any-source multicast (ASM), source-filtered multicast (SFM), and source-specific multicast (SSM).

ASM model

In the ASM model, any sender can send information to a multicast group as a multicast source, and receivers can join a multicast group (identified by a group address) and obtain multicast information addressed to that multicast group. In this model, receivers do not know the positions of the multicast sources in advance. However, they can join or leave the multicast group at any time.

SFM model

The SFM model is derived from the ASM model. To a sender, the two models appear to have the same multicast membership architecture.

The SFM model functionally extends the ASM model. The upper-layer software checks the source address of received multicast packets and permits or denies multicast traffic from specific sources. Therefore, receivers can receive the multicast data from only part of the multicast sources. To a receiver, multicast sources are not all valid; they are filtered.

SSM model

Users might be interested in the multicast data from only certain multicast sources. The SSM model provides a transmission service that enables users to specify the multicast sources that they are interested in at the client side.

The main difference between the SSM model and the ASM model is that in the SSM model, receivers have already determined the locations of the multicast sources by some other means. In addition, the SSM model uses a multicast address range that is different from that of the ASM/SFM model, and dedicated multicast forwarding paths are established between receivers and the specified multicast sources.

Multicast architecture

IP multicast addresses the following questions:

- Where should the multicast source transmit information to? (Multicast addressing.)
- What receivers exist on the network? (Host registration.)
- Where is the multicast source that will provide data to the receivers? (Multicast source discovery.)
- How should information be transmitted to the receivers? (Multicast routing.)

IP multicast is an end-to-end service. The multicast architecture involves the following parts:

- **Addressing mechanism**—A multicast source sends information to a group of receivers through a multicast address.
- **Host registration**—Receiver hosts can join and leave multicast groups dynamically. This mechanism is the basis for management of group memberships.
- **Multicast routing**—A multicast distribution tree (a forwarding path tree for multicast data on the network) is constructed for delivering multicast data from a multicast source to receivers.
- **Multicast applications**—A software system that supports multicast applications, such as video conferencing, must be installed on multicast sources and receiver hosts. The TCP/IP stack must support reception and transmission of multicast data.

Multicast addresses

Network-layer multicast addresses (multicast IP addresses) enables communication between multicast sources and multicast group members. In addition, a technique must be available to map multicast IP addresses to link-layer multicast MAC addresses.

IP multicast addresses

- IPv4 multicast addresses
Internet Assigned Numbers Authority (IANA) assigned the Class D address space (224.0.0.0 to 239.255.255.255) to IPv4 multicast.

Table 2 Class D IP address blocks and description

Address block	Description
224.0.0.0 to 224.0.0.255	Reserved permanent group addresses. The IP address 224.0.0.0 is reserved. Other IP addresses can be used by routing protocols and for topology searching, protocol maintenance, and so on. Table 3 lists common permanent group addresses. A packet destined for an address in this block will not be forwarded beyond the local subnet regardless of the Time to Live (TTL) value in the IP header.
224.0.1.0 to 238.255.255.255	Globally scoped group addresses. This block includes the following types of designated group addresses: <ul style="list-style-type: none">• 232.0.0.0/8—SSM group addresses.• 233.0.0.0/8—Glop group addresses.

Address block	Description
239.0.0.0 to 239.255.255.255	Administratively scoped multicast addresses. These addresses are considered locally unique rather than globally unique, and can be reused in domains administered by different organizations without causing conflicts. For more information, see RFC 2365.

NOTE:

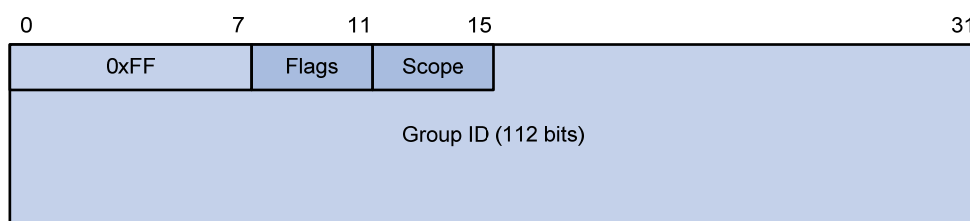
"Glop" is a mechanism for assigning multicast addresses between different autonomous systems (ASs). By filling an AS number into the middle two bytes of 233.0.0.0, you get 255 multicast addresses for that AS. For more information, see RFC 2770.

Table 3 Some reserved multicast addresses

Address	Description
224.0.0.1	All systems on this subnet, including hosts and routers
224.0.0.2	All multicast routers on this subnet
224.0.0.3	Unassigned
224.0.0.4	Distance Vector Multicast Routing Protocol (DVMRP) routers
224.0.0.5	Open Shortest Path First (OSPF) routers
224.0.0.6	OSPF designated routers and backup designated routers
224.0.0.7	Shared Tree (ST) routers
224.0.0.8	ST hosts
224.0.0.9	Routing Information Protocol version 2 (RIPv2) routers
224.0.0.11	Mobile agents
224.0.0.12	Dynamic Host Configuration Protocol (DHCP) server/relay agent
224.0.0.13	All Protocol Independent Multicast (PIM) routers
224.0.0.14	Resource Reservation Protocol (RSVP) encapsulation
224.0.0.15	All Core-Based Tree (CBT) routers
224.0.0.16	Designated Subnetwork Bandwidth Management (SBM)
224.0.0.17	All SBMs
224.0.0.18	Virtual Router Redundancy Protocol (VRRP)

- IPv6 multicast addresses

Figure 4 IPv6 multicast format



The following describes the fields of an IPv6 multicast address:

- **0xFF**—The most significant eight bits are 11111111, which indicates that this address is an IPv6 multicast address.
- **Flags**—The Flags field contains four bits.

Figure 5 Flags field format



Table 4 Flags field description

Bit	Description
0	Reserved, set to 0.
R	<ul style="list-style-type: none"> • When set to 0, it indicates that this address is an IPv6 multicast address without an embedded RP address. • When set to 1, it indicates that this address is an IPv6 multicast address with an embedded RP address. (The P and T bits must also be set to 1.)
P	<ul style="list-style-type: none"> • When set to 0, it indicates that this address is an IPv6 multicast address not based on a unicast prefix. • When set to 1, it indicates that this address is an IPv6 multicast address based on a unicast prefix. (The T bit must also be set to 1.)
T	<ul style="list-style-type: none"> • When set to 0, it indicates that this address is an IPv6 multicast address permanently-assigned by IANA. • When set to 1, it indicates that this address is a transient, or dynamically assigned IPv6 multicast address.

- **Scope**—The Scope field contains four bits, which indicate the scope of the IPv6 internetwork for which the multicast traffic is intended.

Table 5 Values of the Scope field

Value	Meaning
0, F	Reserved
1	Interface-local scope
2	Link-local scope
3	Subnet-local scope
4	Admin-local scope
5	Site-local scope
6, 7, 9 through D	Unassigned
8	Organization-local scope
E	Global scope

- **Group ID**—The Group ID field contains 112 bits. It uniquely identifies an IPv6 multicast group in the scope that the Scope field defines.

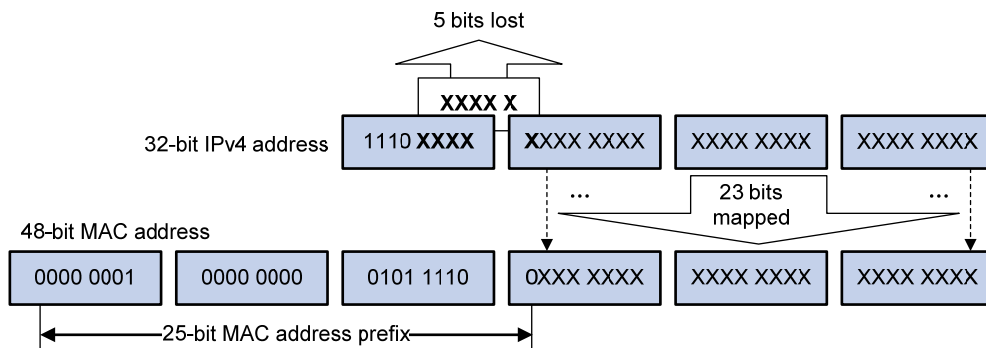
Ethernet multicast MAC addresses

A multicast MAC address identifies a group of receivers at the data link layer.

- IPv4 multicast MAC addresses

As defined by IANA, the most significant 24 bits of an IPv4 multicast MAC address are 0x01005E. Bit 25 is 0, and the other 23 bits are the least significant 23 bits of a multicast IPv4 address.

Figure 6 IPv4-to-MAC address mapping

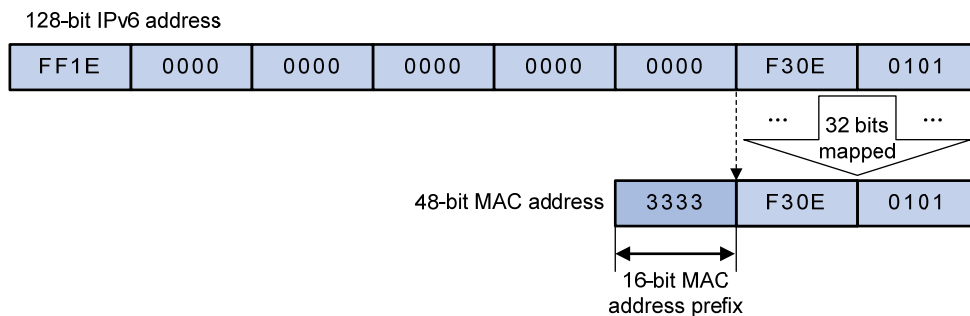


The most significant four bits of a multicast IPv4 address are 1110, which indicates that this address is a multicast address. Only 23 bits of the remaining 28 bits are mapped to a MAC address, so five bits of the multicast IPv4 address are lost. As a result, 32 multicast IPv4 addresses map to the same IPv4 multicast MAC address. Therefore, in Layer 2 multicast forwarding, a switch might receive some multicast data destined for other IPv4 multicast groups. The upper layer must filter such redundant data.

- IPv6 multicast MAC addresses

The most significant 16 bits of an IPv6 multicast MAC address are 0x3333. The least significant 32 bits are the least significant 32 bits of a multicast IPv6 address.

Figure 7 An example of IPv6-to-MAC address mapping



Multicast protocols

Generally, Layer 3 multicast refers to IP multicast working at the network layer. The corresponding multicast protocols are Layer 3 multicast protocols, which include IGMP, MLD, PIM, IPv6 PIM, MSDP, MBGP, and IPv6 MBGP. Layer 2 multicast refers to IP multicast working at the data link layer. The corresponding multicast protocols are Layer 2 multicast protocols, which include IGMP snooping, MLD snooping, PIM snooping, IPv6 PIM snooping, multicast VLAN, and IPv6 multicast VLAN.

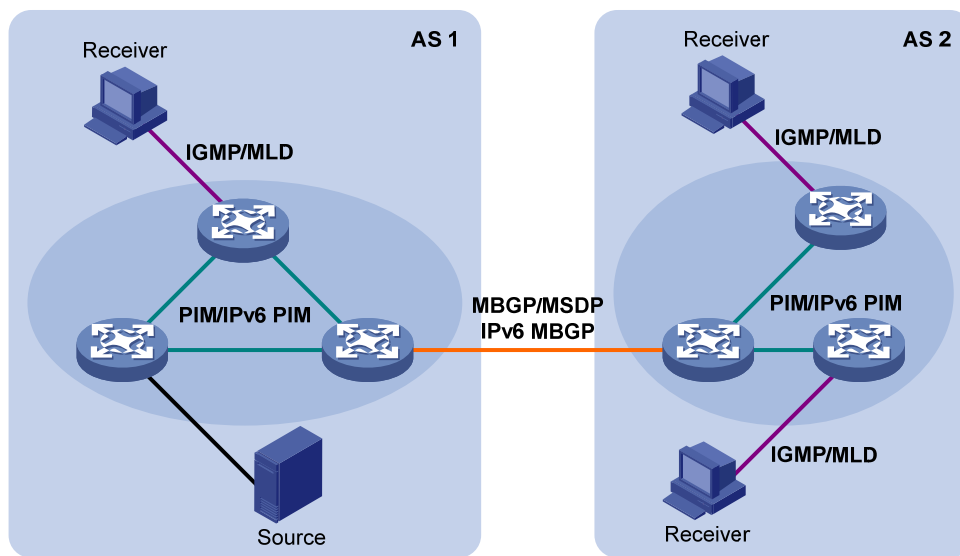
IGMP snooping, PIM snooping, multicast VLAN, IGMP, PIM, MSDP, and MBGP are for IPv4, and MLD snooping, IPv6 PIM snooping, IPv6 multicast VLAN, MLD, IPv6 PIM, and IPv6 MBGP are for IPv6.

This section provides only general descriptions about applications and functions of the Layer 2 and Layer 3 multicast protocols in a network. For more information about these protocols, see the related chapters.

Layer 3 multicast protocols

Layer 3 multicast protocols include multicast group management protocols and multicast routing protocols.

Figure 8 Positions of Layer 3 multicast protocols



- Multicast group management protocols
Typically, the Internet Group Management Protocol (IGMP) or Multicast Listener Discovery Protocol (MLD) is used between hosts and Layer 3 multicast devices that directly connect to the hosts. These protocols define the mechanism of establishing and maintaining group memberships between hosts and Layer 3 multicast devices.
- Multicast routing protocols
A multicast routing protocol runs on Layer 3 multicast devices to establish and maintain multicast routes and forward multicast packets correctly and efficiently. Multicast routes constitute loop-free data transmission paths from a data source to multiple receivers, namely, a multicast distribution tree.

In the ASM model, multicast routes include intra-domain routes and inter-domain routes.

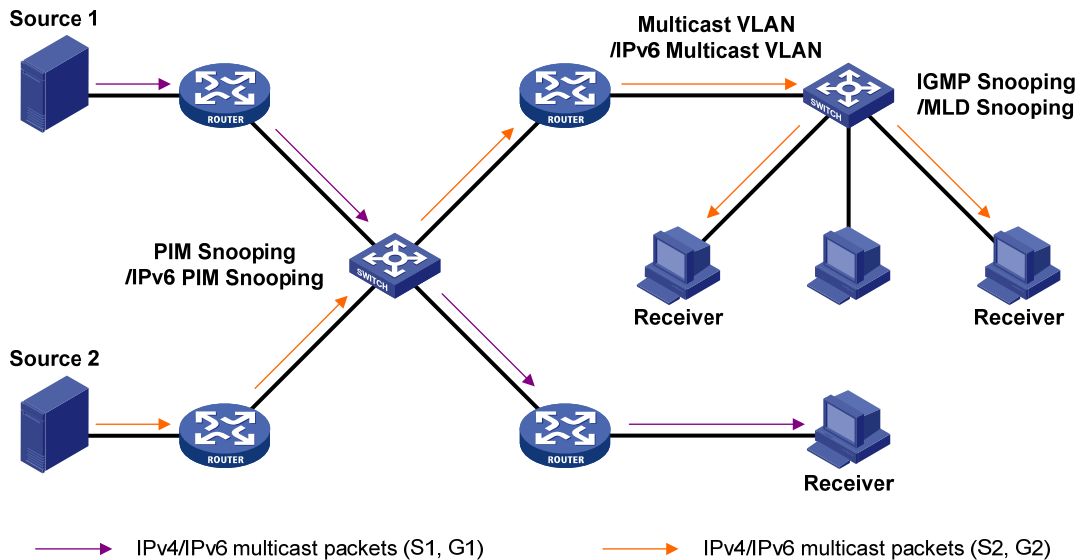
- An intra-domain multicast routing protocol discovers multicast sources and builds multicast distribution trees within an AS to deliver multicast data to receivers. Among a variety of mature intra-domain multicast routing protocols, Protocol Independent Multicast (PIM) is most widely used. Based on the forwarding mechanism, PIM has dense mode (often referred to as "PIM-DM"), and sparse mode (often referred to as "PIM-SM").
- An inter-domain multicast routing protocol is used for delivery of multicast information between two ASs. So far, mature solutions include Multicast Source Discovery Protocol (MSDP) and Multicast Border Gateway Protocol (MBGP). MSDP propagates multicast source information among different ASs. MBGP is an extension of the Multiprotocol Border Gateway Protocol (MP-BGP) for exchanging multicast routing information among different ASs.

For the SSM model, multicast routes are not divided into intra-domain routes and inter-domain routes. Because receivers know the position of the multicast source, channels established through PIM-SM are sufficient for the transport of multicast information.

Layer 2 multicast protocols

Layer 2 multicast protocols include IGMP snooping, MLD snooping, PIM snooping, IPv6 PIM snooping, multicast VLAN, and IPv6 multicast VLAN.

Figure 9 Positions of Layer 2 multicast protocols



- IGMP snooping and MLD snooping
IGMP snooping and MLD snooping are multicast constraining mechanisms that run on Layer 2 devices. They manage and control multicast groups by monitoring and analyzing IGMP or MLD messages exchanged between the hosts and Layer 3 multicast devices, effectively controlling the flooding of multicast data in a Layer 2 network.
- PIM snooping and IPv6 PIM snooping

PIM snooping and IPv6 PIM snooping run on Layer 2 devices. They determine which ports are interested in multicast data by analyzing the received IPv6 PIM messages, and add the ports to a multicast forwarding entry to make sure that multicast data can be forwarded to only the ports that are interested in the data.

- Multicast VLAN and IPv6 multicast VLAN

In the traditional multicast-on-demand mode, when users in different VLANs on a Layer 2 device need multicast information, the upstream Layer 3 device must forward a separate copy of the multicast data to each VLAN of the Layer 2 device. When the multicast VLAN or IPv6 multicast VLAN feature is enabled on the Layer 2 device, the Layer 3 multicast device sends only one copy of multicast to the multicast VLAN or IPv6 multicast VLAN on the Layer 2 device. This approach avoids waste of network bandwidth and extra burden on the Layer 3 device.

Multicast packet forwarding mechanism

In a multicast model, a multicast source sends information to the host group identified by the multicast group address in the destination address field of IP multicast packets. To deliver multicast packets to receivers located at different positions of the network, multicast routers on the forwarding paths usually need to forward multicast packets that an incoming interface receives to multiple outgoing interfaces. Compared with a unicast model, a multicast model is more complex in the following aspects:

- To ensure multicast packet transmission in the network, unicast routing tables or multicast routing tables (for example, the MBGP routing table) specially provided for multicast must be used as guidance for multicast forwarding.
- To process the same multicast information from different peers received on different interfaces of the same device, every multicast packet undergoes a reverse path forwarding (RPF) check on the incoming interface. The result of the RPF check determines whether the packet will be forwarded or discarded. The RPF check mechanism is the basis for most multicast routing protocols to implement multicast forwarding.

For more information about the RPF mechanism, see "[Configuring multicast routing and forwarding \(available only on the HP 5500 EI\)](#)" and "[Configuring IPv6 multicast routing and forwarding \(available only on the HP 5500 EI\)](#)."

Multicast support for VPNs

Multicast support for VPNs refers to multicast applied in virtual private networks (VPNs).

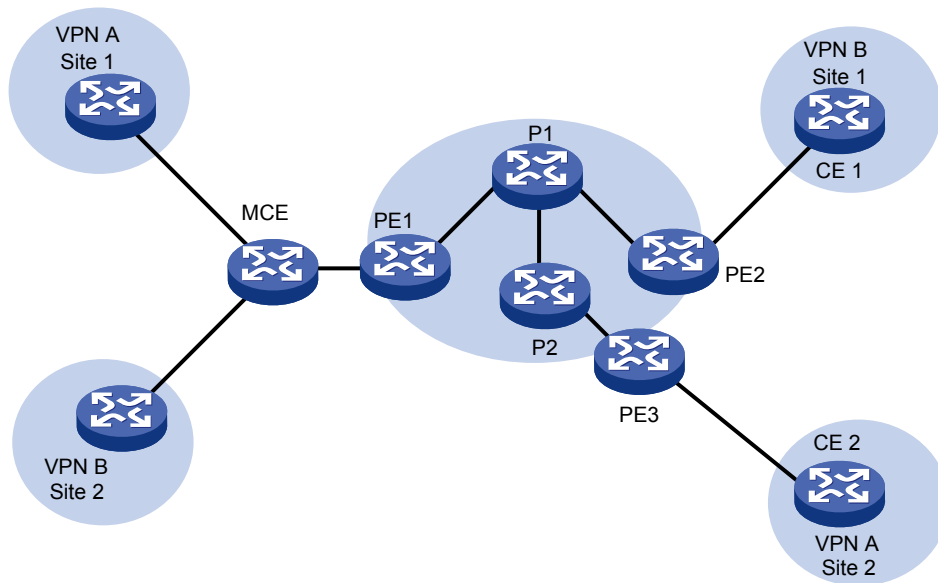
NOTE:

- Multicast support for VPNs is not available in IPv6 networks.
 - Multicast supporting for VPNs is not available for the HP 5500 SI switches.
-

Introduction to VPN instances

VPNs must be isolated from one another and from the public network. As shown in Figure 10, VPN A and VPN B separately access the public network through PE devices.

Figure 10 VPN networking diagram



- The provider (P) device belongs to the public network. The customer edge (CE) devices belong to their respective VPNs. Each P device and CE device serves its own VPN and maintains only one set of forwarding mechanisms.
- The multi-VPN-instance customer edge (MCE) device connects to the VPNs and PE devices and serves multiple VPNs. Different VPN instances for VPNs can be created on the MCE device to separately maintain their forwarding tables.
- The provider edge (PE) devices connect to the public network and the VPNs and serve multiple networks. Multiple instances can exist on the same PE device. On a PE device, the instance for the public network is called the public network instance, and those for VPNs are called VPN instances.

NOTE:

The HP 5500 EI switches can act as MCE or CE devices.

Multicast application in VPNs

A PE or MCE device that supports multicast for VPNs does the following operations:

- Maintains an independent set of multicast forwarding mechanisms for each VPN, including the multicast protocols, PIM neighbor information, and multicast routing table. In a VPN, the device forwards multicast data based on the forwarding table or routing table for that VPN.
- Implements the isolation between different VPNs.

The PE device also implements information exchange and data conversion between the public network and VPN instances.

As shown in [Figure 10](#), when a multicast source in VPN A sends a multicast stream to a multicast group, only the receivers that belong to both the multicast group and VPN A can receive the multicast stream. The multicast data is multicast both in VPN A and on the public network.

Configuring IGMP snooping

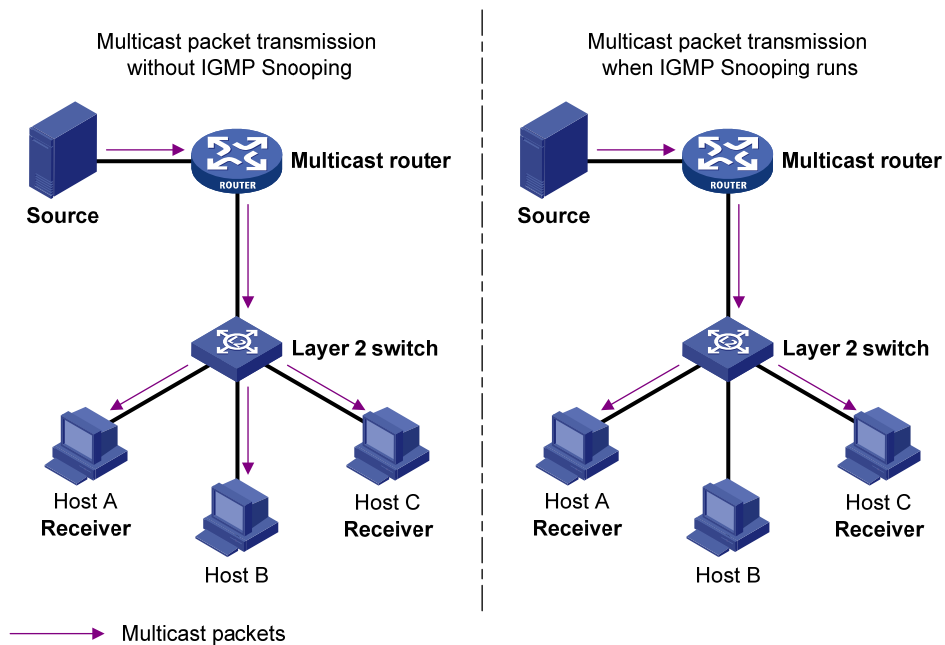
Overview

Internet Group Management Protocol (IGMP) snooping is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

By analyzing received IGMP messages, a Layer 2 device that runs IGMP snooping establishes mappings between ports and multicast MAC addresses, and forwards multicast data based on these mappings.

As shown in [Figure 11](#), without IGMP snooping enabled, the Layer 2 switch floods multicast packets to all devices at Layer 2. With IGMP snooping enabled, the Layer 2 switch forwards multicast packets for known multicast groups to only the receivers that require the multicast data at Layer 2. This feature improves bandwidth efficiency, enhances multicast security, and helps per-host accounting for multicast users.

Figure 11 Before and after IGMP snooping is enabled on the Layer 2 device

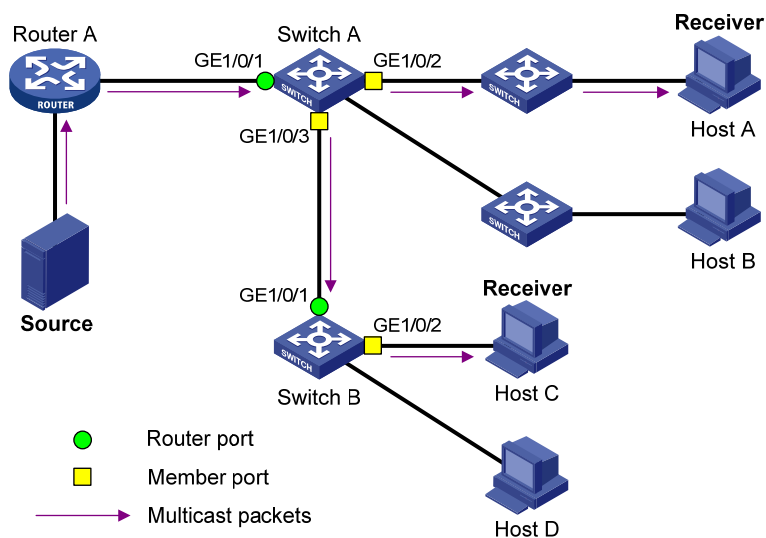


Basic concepts in IGMP snooping

IGMP snooping related ports

As shown in [Figure 12](#), Router A connects to the multicast source, IGMP snooping runs on Switch A and Switch B, and Host A and Host C are receiver hosts as members of a multicast group.

Figure 12 IGMP snooping related ports



The following describes the ports involved in IGMP snooping:

- **Router port**—Layer 3 multicast device-side port. Layer 3 multicast devices include designated routers (DRs) and IGMP queriers. In Figure 12, GigabitEthernet 1/0/1 of Switch A and GigabitEthernet 1/0/1 of Switch B are router ports. The switch registers all its router ports in its router port list.
Do not confuse the "router port" in IGMP snooping with the "routed interface" commonly known as the "Layer 3 interface." The router port in IGMP snooping is the Layer 2 interface.
- **Member port**—Multicast receiver-side port. In Figure 12, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and GigabitEthernet 1/0/2 of Switch B are member ports. The switch registers all its member ports in its IGMP snooping forwarding table.

Unless otherwise specified, router ports and member ports in this document include both static and dynamic router ports and member ports.

NOTE:

An IGMP-snooping-enabled switch deems that all its ports on which IGMP general queries with the source IP address other than 0.0.0.0 or that receive PIM hello messages are received are dynamic router ports. For more information about PIM hello messages, see "[Configuring PIM \(available only on the HP 5500 E1\)](#)."

Aging timers for dynamic ports in IGMP snooping and related messages and actions

Timer	Description	Message before expiry	Action after expiry
Dynamic router port aging timer	For each dynamic router port, the switch starts an aging timer. When the timer expires, the dynamic router port ages out.	IGMP general query of which the source address is not 0.0.0.0 or PIM hello.	The switch removes this port from its router port list.
Dynamic member port aging timer	When a port dynamically joins a multicast group, the switch starts an aging timer for the port. When the timer expires, the dynamic member port ages out.	IGMP membership report.	The switch removes this port from the IGMP snooping forwarding table.

NOTE:

In IGMP snooping, only dynamic ports age out. Static ports never age out.

How IGMP snooping works

In this section, the involved ports are dynamic ports. For information about how to configure and remove static ports, see "[Configuring static ports](#)."

A switch that runs IGMP snooping performs different actions when it receives different IGMP messages.

When receiving a general query

The IGMP querier periodically sends IGMP general queries to all hosts and routers identified by the address 224.0.0.1 on the local subnet to determine whether any active multicast group members exist on the subnet.

After receiving an IGMP general query, the switch forwards it to all ports in the VLAN, except the port that received the query. The switch also performs one of the following actions:

- If the receiving port is a dynamic router port in the router port list, restarts the aging timer for the port.
- If the receiving port is not in its router port list, adds it into its router port list as a dynamic router port and starts an aging timer for the port.

When receiving a membership report

A host sends an IGMP report to the IGMP querier for the following purposes:

- If the host has been a member of a multicast group, responds to the query with an IGMP report.
- Applies for joining a multicast group.

After receiving an IGMP report, the switch forwards it through all the router ports in the VLAN, resolves the address of the reported multicast group. The switch also performs one of the following actions:

- If no forwarding entry matches the group address, creates a forwarding entry for the group, adds the receiving port as a dynamic member port to the forwarding entry, and starts an aging timer for the port.
- If a forwarding entry matches the group address, but the receiving port is not in the forwarding entry for the group, adds the port as a dynamic member port to the forwarding entry and starts an aging timer for the port.
- If a forwarding entry matches the group address and the receiving port is in the forwarding entry for the group, restarts the aging timer for the port.

A switch does not forward an IGMP report through a non-router port. If the switch forwards a report message through a member port, the IGMP report suppression mechanism causes all the attached hosts that are monitoring the reported multicast address suppress their own reports. This makes the switch unable to know whether the reported multicast group still has active members attached to that port. For more information about the IGMP report suppression mechanism, see "[Configuring IGMP \(available only on the HP 5500 EI\)](#)."

When receiving a leave message

When an IGMPv1 host leaves a multicast group, the host does not send an IGMP leave message, and the switch cannot know immediately that the host has left the multicast group. However, because the host stops sending IGMP reports as soon as it leaves the multicast group, the switch removes the port that connects to the host from the forwarding entry for the multicast group when the aging timer for the port expires.

When an IGMPv2 or IGMPv3 host leaves a multicast group, the host sends an IGMP leave message to the multicast router.

When the switch receives an IGMP leave message on a dynamic member port, the switch first examines whether a forwarding entry matches the group address in the message, and, if a match is found, whether the forwarding entry for the group contains the dynamic member port.

- If no forwarding entry matches the group address, or if the forwarding entry does not contain the port, the switch directly discards the IGMP leave message.
- If a forwarding entry matches the group address and the forwarding entry contains the port, the switch forwards the leave message to all router ports in the VLAN. Because the switch does not know whether any other hosts attached to the port are still listening to that group address, the switch does not immediately remove the port from the forwarding entry for that group. Instead, it restarts the aging timer for the port.

After receiving the IGMP leave message, the IGMP querier resolves the multicast group address in the message and sends an IGMP group-specific query to the multicast group through the port that received the leave message. After receiving the IGMP group-specific query, the switch forwards it through all its router ports in the VLAN and all member ports of the multicast group. The switch also performs the following judgment for the port that received the IGMP leave message:

- If the port (assuming that it is a dynamic member port) receives an IGMP report in response to the group-specific query before its aging timer expires, it indicates that some host attached to the port

is receiving or expecting to receive multicast data for the multicast group. The switch restarts the aging timer for the port.

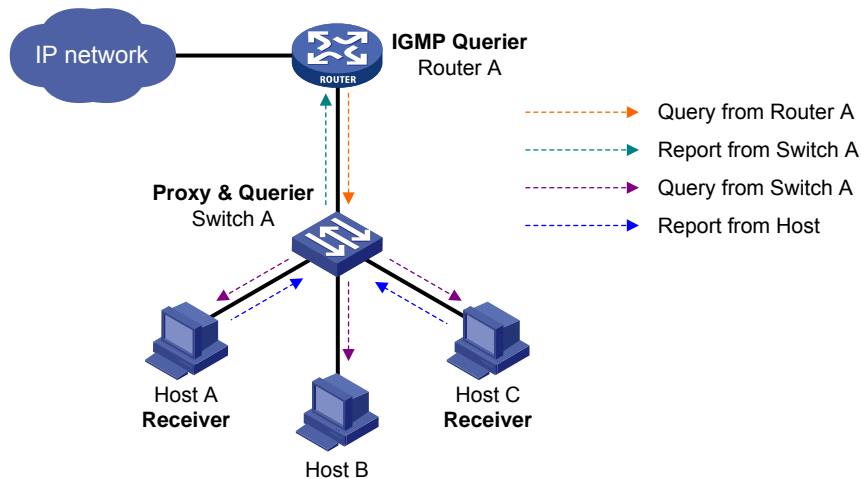
- If the port receives no IGMP report in response to the group-specific query before its aging timer expires, it indicates that no hosts attached to the port are still listening to that group address. The switch removes the port from the forwarding entry for the multicast group when the aging timer expires.

IGMP snooping proxying

You can configure the IGMP snooping proxying function on an edge device to reduce the number of IGMP reports and leave messages sent to its upstream device. The device configured with IGMP snooping proxying is called an IGMP snooping proxy. It is a host from the perspective of its upstream device.

Even though an IGMP snooping proxy is a host from the perspective of its upstream device, the IGMP membership report suppression mechanism for hosts does not take effect on it. For more information about the IGMP report suppression mechanism for hosts, see "[Configuring IGMP \(available only on the HP 5500 EI\)](#)."

Figure 13 Network diagram



As shown in Figure 13, Switch A works as an IGMP snooping proxy. As a host from the perspective of the querier Router A, Switch A represents its attached hosts to send membership reports and leave messages to Router A.

Table 6 IGMP message processing on an IGMP snooping proxy

IGMP message	Actions
General query	When receiving an IGMP general query, the proxy forwards it to all ports but the receiving port. In addition, the proxy generates a report according to the group memberships it maintains and sends the report out of all router ports.

IGMP message	Actions
Group-specific query	In response to the IGMP group-specific query for a certain multicast group, the proxy sends the report to the group out of all router ports if the forwarding entry for the group still contains a member port.
Report	<p>After receiving a report for a multicast group, the proxy looks up the multicast forwarding table for the forwarding entry for the multicast group.</p> <ul style="list-style-type: none"> • If a forwarding entry matches the multicast group and contains the receiving port as a dynamic member port, the proxy restarts the aging timer for the port. • If a forwarding entry matches the multicast group but does not contain the receiving port, the proxy adds the port to the forwarding entry as a dynamic member port and starts an aging timer for the port. • If no forwarding entry matches the multicast group, the proxy creates a forwarding entry for the multicast group, adds the receiving port to the forwarding entry as a dynamic member port, and starts an aging timer for the port.
Leave	In response to an IGMP leave message for a multicast group, the proxy sends a group-specific query out of the receiving port. After making sure that no member port is contained in the forwarding entry for the multicast group, the proxy sends a leave message to the group out of all router ports.

Protocols and standards

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

IGMP snooping configuration task list

Task	Remarks	
Configuring basic IGMP snooping functions	Enabling IGMP snooping	Required
	Specifying the version of IGMP snooping	Optional
	Configuring static multicast MAC address entries	Optional
	Setting aging timers for dynamic ports	Optional
Configuring IGMP snooping port functions	Configuring static ports	Optional
	Configuring a port as a simulated member host	Optional
	Enabling IGMP snooping fast-leave processing	Optional
	Disabling a port from becoming a dynamic router port	Optional
Configuring IGMP snooping querier	Enabling IGMP snooping querier	Optional
	Configuring parameters for IGMP queries and responses	Optional
	Configuring the source IP addresses for IGMP queries	Optional

Task	Remarks	
Configuring IGMP snooping proxying	Enabling IGMP snooping proxying	Optional
	Configuring a source IP address for the IGMP messages sent by the proxy	Optional
Configuring an IGMP snooping policy	Configuring a multicast group filter	Optional
	Configuring multicast source port filtering	Optional
	Enabling dropping unknown multicast data	Optional
	Configuring IGMP report suppression	Optional
	Setting the maximum number of multicast groups that a port can join	Optional
	Setting the 802.1p precedence for IGMP messages	Optional
	Enabling multicast group replacement	Optional
	Configuring a multicast user control policy	Optional
Enabling the IGMP snooping host tracking function	Optional	
Setting the DSCP value for IGMP messages	Optional	

For the configuration tasks in this section:

- In IGMP snooping view, the configurations that you make are effective in all VLANs. In VLAN view, the configurations that you make are effective on only the ports that belong to the current VLAN. For a given VLAN, a configuration that you make in IGMP snooping view is effective only if you do not make the same configuration in VLAN view.
- In IGMP snooping view, the configurations that you make are effective on all ports. In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the configurations that you make are effective only on the current port. In port group view, the configurations that you make are effective on all ports in the current port group. For a given port, a configuration that you make in IGMP snooping view is effective only if you do not make the same configuration in Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.
- For IGMP snooping, the configurations that you make on a Layer 2 aggregate interface do not interfere with those you make on its member ports, nor do they participate in aggregation calculations. Configurations that you make on a member port of an aggregate group do not take effect until it leaves the aggregate group.

Configuring basic IGMP snooping functions

Before you configure basic IGMP snooping functions, complete the following tasks:

- Configure the corresponding VLANs.
- Determine the version of IGMP snooping.

Enabling IGMP snooping

When you enable IGMP snooping, follow these guidelines:

- You must enable IGMP snooping globally before you enable it in a VLAN.
- After you enable IGMP snooping in a VLAN, do not enable IGMP or PIM on the corresponding VLAN interface.
- When you enable IGMP snooping in a specified VLAN, IGMP snooping works only on the ports in this VLAN.

To enable IGMP snooping:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IGMP snooping globally and enter IGMP-snooping view.	igmp-snooping	Disabled by default
3. Return to system view.	quit	N/A
4. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
5. Enable IGMP snooping in the VLAN.	igmp-snooping enable	Disabled by default

Specifying the version of IGMP snooping

Different versions of IGMP snooping can process different versions of IGMP messages:

- IGMPv2 snooping can process IGMPv1 and IGMPv2 messages, but cannot process IGMPv3 messages, which will be flooded in the VLAN.
- IGMPv3 snooping can process IGMPv1, IGMPv2 and IGMPv3 messages.

If you change IGMPv3 snooping to IGMPv2 snooping, the system:

- Clears all IGMP snooping forwarding entries that are dynamically added.
- Keeps static IGMPv3 snooping forwarding entries (*, G).
- Clears static IGMPv3 snooping forwarding entries (S, G), which will be restored when IGMP snooping is switched back to IGMPv3 snooping.

For more information about static joins, see "[Configuring static ports.](#)"

To specify the version of IGMP snooping:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Specify the version of IGMP snooping.	igmp-snooping version <i>version-number</i>	Version 2 by default

Configuring static multicast MAC address entries

In Layer-2 multicast, a Layer 2 multicast protocol (such as IGMP snooping) can dynamically add multicast MAC address entries. Or, you can manually configure multicast MAC address entries.

Configuration guidelines

- In system view, the configuration is effective for the specified ports. In interface view or port group view, the configuration is effective only on the current port or the ports in the current port group.
- Any legal multicast MAC address except 0100-5Exx-xxxx (where "x" represents a hexadecimal number from 0 to F) can be manually added to the multicast MAC address table. Multicast MAC addresses are the MAC addresses whose the least significant bit of the most significant octet is 1.

Configuration procedure

To configure a static multicast MAC address entry in system view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure a static multicast MAC address entry.	mac-address multicast <i>mac-address interface interface-list</i> vlan <i>vlan-id</i>	No static multicast MAC address entries exist by default.

To configure static multicast MAC address entries in interface view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none">• Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type interface-number</i>• Enter port group view: port-group manual <i>port-group-name</i>	Use either command.
3. Configure a static multicast MAC address entry.	mac-address multicast <i>mac-address vlan</i> <i>vlan-id</i>	No static multicast MAC address entries exist by default.

Configuring IGMP snooping port functions

Before you configure IGMP snooping port functions, complete the following tasks:

- Enable IGMP snooping in the VLAN.
- Configure the corresponding port groups.
- Determine the aging time of dynamic router ports.
- Determine the aging time of dynamic member ports.

- Determine the multicast group and multicast source addresses.

Setting aging timers for dynamic ports

If a switch receives no IGMP general queries or PIM hello messages on a dynamic router port when the aging timer of the port expires, the switch removes the port from the router port list.

If the switch receives no IGMP reports for a multicast group on a dynamic member port when the aging timer of the port expires, the switch removes the port from the multicast forwarding entry for that multicast group.

If the memberships of multicast groups change frequently, you can set a relatively small value for the aging timer of the dynamic member ports. If the memberships of multicast groups change rarely, you can set a relatively large value.

Configuring aging timers for dynamic ports globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IGMP-snooping view.	igmp-snooping	N/A
3. Set the aging timer for dynamic router ports.	router-aging-time <i>interval</i>	105 seconds by default
4. Set the aging timer for dynamic member ports.	host-aging-time <i>interval</i>	260 seconds by default

Configuring aging timers for dynamic ports in a VLAN

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Set the aging timer for dynamic router ports.	igmp-snooping router-aging-time <i>interval</i>	105 seconds by default
4. Set the aging timer for dynamic member ports.	igmp-snooping host-aging-time <i>interval</i>	260 seconds by default

Configuring static ports

If all hosts attached to a port are interested in the multicast data addressed to a particular multicast group or the multicast data that a particular multicast source sends to a particular group, you can configure the port as a static member port for the specified multicast group or the specified multicast source and group.

You can also configure a port as a static router port, through which the switch can forward all the multicast traffic that it received.

Configuration guidelines

- A static member port does not respond to queries from the IGMP querier; when you configure a port as a static member port or cancel this configuration on the port, the port does not send an unsolicited IGMP report or an IGMP leave message.
- Static member ports and static router ports never age out. To remove such a port, use the corresponding **undo** command.

Configuration procedure

To configure static ports:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none">• Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i>• Enter port group view: port-group manual <i>port-group-name</i>	Use either command.
3. Configure the port as a static member port.	igmp-snooping static-group <i>group-address</i> [source-ip <i>source-address</i>] vlan <i>vlan-id</i>	No static member ports exist by default.
4. Configure the port as a static router port.	igmp-snooping static-router-port vlan <i>vlan-id</i>	No static router ports exist by default.

Configuring a port as a simulated member host

Generally, a host that runs IGMP can respond to IGMP queries that the IGMP querier sends. If a host fails to respond, the multicast router might deem that no member of this multicast group exists on the network segment, and removes the corresponding forwarding path.

To avoid this situation, you can configure the port as a simulated member host for a multicast group. A simulated host is equivalent to an independent host. For example, when a simulated member host receives an IGMP query, it gives a response separately. Therefore, the switch can continue receiving multicast data.

A simulated host acts like a real host in the following ways:

- When a port is configured as a simulated member host, the switch sends an unsolicited IGMP report through the port, and can respond to IGMP general queries with IGMP reports through the port.
- When the simulated joining function is disabled on a port, the switch sends an IGMP leave message through the port.

Unlike a static member port, a port that you configure as a simulated member host ages out like a dynamic member port.

To configure a port as a simulated member host:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
3. Configure a port as a simulated member host.	igmp-snooping host-join <i>group-address</i> [source-ip <i>source-address</i>] vlan <i>vlan-id</i>	Not configured by default.

Enabling IGMP snooping fast-leave processing

IGMP snooping fast-leave processing enables the switch to process IGMP leave messages quickly. With IGMP snooping fast-leave processing enabled, when the switch receives an IGMP leave message on a port, it immediately removes that port from the forwarding entry for the multicast group specified in the message. Then, when the switch receives IGMP group-specific queries for that multicast group, it does not forward them to that port.

On a port that has only one host attached, you can enable IGMP snooping fast-leave processing to save bandwidth and resources. However, on a port that has multiple hosts attached, you should not enable IGMP snooping fast-leave processing if you have enabled dropping unknown multicast data globally or for the port. Otherwise, if a host on the port leaves a multicast group, the other hosts attached to the port in the same multicast group cannot receive the multicast data for the group.

Enabling IGMP snooping fast-leave processing globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IGMP-snooping view.	igmp-snooping	N/A
3. Enable IGMP snooping fast-leave processing.	fast-leave [vlan <i>vlan-list</i>]	Disabled by default

Enabling IGMP snooping fast-leave processing on a port

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
3. Enable IGMP snooping fast-leave processing.	igmp-snooping fast-leave [vlan <i>vlan-list</i>]	Disabled by default.

Disabling a port from becoming a dynamic router port

The following problems might exist in a multicast access network:

- After receiving an IGMP general query or a PIM hello message from a connected host, a router port becomes a dynamic router port. Before its timer expires, this dynamic router port receives all multicast packets within the VLAN where the port belongs, and forwards them to the host, affecting normal multicast reception of the host.
- In addition, the IGMP general query or PIM hello message that the host sends affects the multicast routing protocol state on Layer 3 devices, such as the IGMP querier or DR election, and might further cause network interruption.

To solve these problems, disable that router port from becoming a dynamic router port after the port receives an IGMP general query or a PIM hello message, so as to improve network security and control over multicast users.

To disable a port from becoming a dynamic router port:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
3. Disable the ports from becoming dynamic router port.	igmp-snooping router-port-deny [vlan <i>vlan-list</i>]	By default, a port can become a dynamic router port.

NOTE:

This configuration does not affect the static router port configuration.

Configuring IGMP snooping querier

Before you configure IGMP snooping querier, complete the following tasks:

- Enable IGMP snooping in the VLAN.
- Determine the IGMP general query interval.
- Determine the IGMP last-member query interval.
- Determine the maximum response delay for IGMP general queries.
- Determine the source address of IGMP general queries.
- Determine the source address of IGMP group-specific queries.

Enabling IGMP snooping querier

In an IP multicast network that runs IGMP, a multicast router or Layer 3 multicast switch sends IGMP queries, so that all Layer 3 multicast devices can establish and maintain multicast forwarding entries, in order to forward multicast traffic correctly at the network layer. This router or Layer 3 switch is called the "IGMP querier." For more information about IGMP querier, see "[Configuring IGMP \(available only on the HP 5500 EI\)](#)."

However, a Layer 2 multicast switch does not support IGMP, and therefore cannot send general queries by default. When you enable IGMP snooping querier on a Layer 2 switch in a VLAN where multicast traffic is switched only at Layer 2 and no multicast routers are present, the Layer 2 switch sends IGMP queries, so that multicast forwarding entries can be established and maintained at the data link layer.

To enable IGMP snooping querier:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Enable IGMP snooping querier.	igmp-snooping querier	Disabled by default

⚠ IMPORTANT:

In a multicast network that runs IGMP, you do not need to configure an IGMP snooping querier because it may affect IGMP querier elections by sending IGMP general queries with a low source IP address.

Configuring parameters for IGMP queries and responses

⚠ CAUTION:

In the configuration, make sure that the IGMP general query interval is larger than the maximum response delay for IGMP general queries. Otherwise, multicast group members might be deleted by mistake.

You can modify the IGMP general query interval based on actual condition of the network.

A multicast listening host starts a timer for each multicast group that it has joined when it receives an IGMP query (general query or group-specific query). This timer is initialized to a random value in the range of 0 to the maximum response delay advertised in the IGMP query message. When the timer value decreases to 0, the host sends an IGMP report to the multicast group.

To speed up the response of hosts to IGMP queries and avoid simultaneous timer expirations causing IGMP report traffic bursts, you must properly set the maximum response delay.

- The maximum response delay for IGMP general queries is set by the **max-response-time** command.
- The maximum response delay for IGMP group-specific queries equals the IGMP last-member query interval.

Configuring the global parameters for IGMP queries and responses

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IGMP-snooping view.	igmp-snooping	N/A
3. Set the maximum response delay for IGMP general queries.	max-response-time <i>interval</i>	10 seconds by default
4. Set the IGMP last-member query interval.	last-member-query-interval <i>interval</i>	1 second by default

Configuring the parameters for IGMP queries and responses in a VLAN

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Set the interval for sending IGMP general queries.	igmp-snooping query-interval <i>interval</i>	60 seconds by default
4. Set the maximum response delay for IGMP general queries.	igmp-snooping max-response-time <i>interval</i>	10 seconds by default
5. Set the IGMP last-member query interval.	igmp-snooping last-member-query-interval <i>interval</i>	1 second by default

Configuring the source IP addresses for IGMP queries

After the switch receives an IGMP query whose source IP address is 0.0.0.0 on a port, it does not enlist that port as a dynamic router port. This might prevent multicast forwarding entries from being correctly created at the data link layer and eventually cause multicast traffic forwarding to fail. To avoid this problem, when a Layer 2 switch acts as the IGMP snooping querier, HP recommends you to configure a non-all-zero IP address as the source IP address of IGMP queries.

❗ **IMPORTANT:**

The source address of IGMP query messages might affect the IGMP querier election within the segment

To configure the source IP addresses for IGMP queries:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Configure the source address of IGMP general queries.	igmp-snooping general-query source-ip { <i>ip-address</i> current-interface }	0.0.0.0 by default
4. Configure the source IP address of IGMP group-specific queries.	igmp-snooping special-query source-ip { <i>ip-address</i> current-interface }	0.0.0.0 by default

Configuring IGMP snooping proxying

Before you configure IGMP snooping proxying in a VLAN, complete the following tasks:

- Enable IGMP snooping in the VLAN.
- Determine the source IP address for the IGMP reports sent by the proxy.
- Determine the source IP address for the IGMP leave messages sent by the proxy.

Enabling IGMP snooping proxying

The IGMP snooping proxying function works on a per-VLAN basis. After you enable the function in a VLAN, the device works as the IGMP snooping proxy for the downstream hosts and upstream router in the VLAN.

To enable IGMP snooping proxying in a VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Enable IGMP snooping proxying in the VLAN.	igmp-snooping proxying enable	Disabled by default

Configuring a source IP address for the IGMP messages sent by the proxy

You can set the source IP addresses in the IGMP reports and leave messages that the IGMP snooping proxy sends on behalf of its attached hosts.

To configure the source IP addresses for the IGMP messages that the IGMP snooping proxy sends on behalf of its attached hosts in a VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Configure a source IP address for the IGMP reports that the proxy sends.	igmp-snooping report source-ip { <i>ip-address</i> current-interface }	The default is 0.0.0.0.
4. Configure a source IP address for the IGMP leave messages that the proxy sends.	igmp-snooping leave source-ip { <i>ip-address</i> current-interface }	The default is 0.0.0.0.

Configuring an IGMP snooping policy

Before you configure an IGMP snooping policy, complete the following tasks:

- Enable IGMP snooping in the VLAN.
- Determine the ACL rule for multicast group filtering.
- Determine the maximum number of multicast groups that a port can join.
- Determine the 802.1p precedence for IGMP messages.

Configuring a multicast group filter

On an IGMP snooping-enabled switch, you can configure a multicast group filter to limit multicast programs available to users.

In an application, when a user requests a multicast program, the user's host initiates an IGMP report. After receiving this report message, the switch resolves the multicast group address in the report and looks up the ACL. If a match is found to permit the port that received the report to join the multicast group, the switch creates an IGMP snooping forwarding entry for the multicast group and adds the port to the forwarding entry. Otherwise, the switch drops this report message, in which case, the multicast data for the multicast group is not sent to this port, and the user cannot retrieve the program.

Configuration guidelines

- When you configure a multicast group filter in a multicast VLAN, be sure to configure the filter in the sub-VLANs of the multicast VLAN. Otherwise, the configuration does not take effect.
- In a network that runs IGMPv3, when a host joins multiple multicast groups, the multicast group filter cannot correctly filter multicast groups because the host that runs IGMPv3 sends multiple multicast groups that it wants to join in one membership report.

Configuration procedure

To configure a multicast group filter globally:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IGMP-snooping view.	igmp-snooping	N/A
3. Configure a multicast group filter.	group-policy <i>acl-number</i> [vlan <i>vlan-list</i>]	By default, no group filter is globally configured. That is, the hosts in a VLAN can join any valid multicast group.

To configure a multicast group filter on a port:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
3. Configure a multicast group filter.	igmp-snooping group-policy <i>acl-number</i> [vlan <i>vlan-list</i>]	By default, no group filter is configured on the current port. That is, the hosts on this port can join any valid multicast group.

Configuring multicast source port filtering

When the multicast source port filtering feature is enabled on a port, the port can connect to only multicast receivers rather than to multicast sources, because the port blocks all multicast data packets but it permits multicast protocol packets to pass.

If this feature is disabled on a port, the port can connect to both multicast sources and multicast receivers.

Configuring multicast source port filtering globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IGMP-snooping view.	igmp-snooping	N/A
3. Enable multicast source port filtering.	source-deny port <i>interface-list</i>	Disabled by default

Configuring multicast source port filtering on a port

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view or port group view.	<ul style="list-style-type: none">Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i>Enter port group view: port-group manual <i>port-group-name</i>	Use either command.
3. Enable multicast source port filtering.	igmp-snooping source-deny	Disabled by default.

Enabling dropping unknown multicast data

Unknown multicast data refers to multicast data for which no entries exist in the IGMP snooping forwarding table. When the switch receives such multicast traffic, one of the following occurs:

- When the function of dropping unknown multicast data is disabled, the switch floods unknown multicast data in the VLAN that the unknown multicast data belongs to, causing network bandwidth waste and low forwarding efficiency.
- When the function of dropping unknown multicast data is enabled, the switch forwards unknown multicast data to its router ports instead of flooding it in the VLAN. If no router ports exist, the switch drops the unknown multicast data.

Configuration procedure

To enable dropping unknown multicast data in a VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Enable dropping unknown multicast data.	igmp-snooping drop-unknown	Disabled by default

Configuring IGMP report suppression

When a Layer 2 switch receives an IGMP report from a multicast group member, the switch forwards the message to the Layer 3 device that directly connects to the Layer 2 switch. When multiple members of a multicast group are attached to the Layer 2 switch, the Layer 3 device might receive duplicate IGMP reports for the multicast group from these members.

With the IGMP report suppression function enabled, within each query interval, the Layer 2 switch forwards only the first IGMP report for the multicast group to the Layer 3 device. It does not forward the subsequent IGMP reports for the same multicast group. This helps reduce the number of packets being transmitted over the network.

❗ **IMPORTANT:**

On an IGMP snooping proxy, IGMP membership reports are suppressed if the entries for the corresponding groups exist in the forwarding table, no matter the suppression function is enabled or not.

To configure IGMP report suppression:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IGMP-snooping view.	igmp-snooping	N/A
3. Enable IGMP report suppression.	report-aggregation	Enabled by default

Setting the maximum number of multicast groups that a port can join

To regulate multicast traffic on a port, configure the maximum number of multicast groups that the port can join.

When you configure this maximum number, if the number of multicast groups the port has joined exceeds the configured maximum value, the system deletes all the forwarding entries for the port from the IGMP snooping forwarding table, and the hosts on this port join multicast groups again until the number of multicast groups that the port joins reaches the maximum value. When the port joins a multicast group, if the port has been configured as a static member port, the system applies the configurations to the port again. If you have configured simulated joining on the port, the system establishes corresponding forwarding entry for the port after receiving a report from the simulated member host.

To set the maximum number of multicast groups that a port can join:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none"> • Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> • Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.

Step	Command	Remarks
3. Set the maximum number of multicast groups that a port can join.	igmp-snooping group-limit <i>limit</i> [vlan <i>vlan-list</i>]	By default, the upper limit is 2000 for the HP 5500 EI switches, and 1000 for the HP 5500 SI switches.

Enabling multicast group replacement

For various reasons, the number of multicast groups that the switch or a port joins might exceed the upper limit. In addition, in some specific applications, a multicast group that the switch newly joins must replace an existing multicast group automatically. A typical example is channel switching. To view a new channel, a user switches from the current multicast group to the new one.

To realize such requirements, you can enable the multicast group replacement function on the switch or on a certain port. When the number of multicast groups that the switch or on the port has joined reaches the limit, one of the following occurs:

- If the multicast group replacement feature is disabled, new IGMP reports are automatically discarded.
- If the multicast group replacement feature is enabled, the multicast group that the switch or a port newly joins automatically replaces an existing multicast group that has the lowest address.

ⓘ IMPORTANT:

In the configuration, be sure to configure the maximum number of multicast groups allowed on a port (see "[Setting the maximum number of multicast groups that a port can join](#)") before enabling multicast group replacement. Otherwise, the multicast group replacement functionality will not take effect.

Enabling multicast group replacement globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IGMP-snooping view.	igmp-snooping	N/A
3. Enable multicast group replacement.	overflow-replace [vlan <i>vlan-list</i>]	Disabled by default

Enabling multicast group replacement on a port

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
3. Enable multicast group replacement.	igmp-snooping overflow-replace [vlan <i>vlan-list</i>]	Disabled by default.

Setting the 802.1p precedence for IGMP messages

You can change the 802.1p precedence for IGMP messages so that they can be assigned higher forwarding priority when congestion occurs on their outgoing ports.

Setting the 802.1p precedence for IGMP messages globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IGMP-snooping view.	igmp-snooping	N/A
3. Set the 802.1p precedence for IGMP messages.	dot1p-priority <i>priority-number</i>	The default 802.1p precedence for IGMP messages is 0.

Setting the 802.1p precedence for IGMP messages in a VLAN

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Set the 802.1p precedence for IGMP messages in the VLAN.	igmp-snooping dot1p-priority <i>priority-number</i>	The default 802.1p precedence for IGMP messages is 0.

Configuring a multicast user control policy

Multicast user control policies are configured on access switches to allow only authorized users to receive requested multicast traffic flows. This helps restrict users from ordering certain multicast-on-demand programs.

In practice, a device first needs to perform authentication (802.1X authentication, for example) on connected hosts through a RADIUS server. Then, the device uses the configured multicast user control policy to perform multicast access control on authenticated users as follows:

- After receiving an IGMP report from a host, the access switch matches the multicast group address and multicast source address carried in the report with the configured policies. If a match is found, the host is allowed to join the multicast group. Otherwise, the join report is dropped by the access switch.
- After receiving an IGMP leave message from a host, the access switch matches the multicast group and source addresses with the policies. If a match is found, the host is allowed to leave the group. Otherwise, the leave message is dropped by the access switch.

A multicast user control policy is functionally similar to a multicast group filter. A difference is that a control policy can control both multicast joining and leaving of users based on authentication and authorization, but a multicast group filter is configured on a port to control only multicast joining but not leaving of users without authentication or authorization.

To configure a multicast user control policy:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a user profile and enter its view.	user-profile <i>profile-name</i>	N/A
3. Configure a multicast user control policy.	igmp-snooping access-policy <i>acl-number</i>	No policy is configured by default. That is, a host can join or leave a valid multicast group at any time.
4. Return to system view.	quit	N/A
5. Enable the created user profile.	user-profile <i>profile-name</i> enable	Disabled by default.

For more information about the **user-profile** and **user-profile enable** commands, see *Security Command Reference*.

Enabling the IGMP snooping host tracking function

With the IGMP snooping host tracking function, the switch can record the information of the member hosts that are receiving multicast traffic, including the host IP address, running duration, and timeout time. You can monitor and manage the member hosts according to the recorded information.

Enabling the IGMP snooping host tracking function globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IGMP-snooping view.	igmp-snooping	N/A
3. Enable the IGMP snooping host tracking function globally.	host-tracking	Disabled by default

Enabling the IGMP snooping host tracking function in a VLAN

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Enable the IGMP snooping host tracking function in the VLAN.	igmp-snooping host-tracking	Disabled by default

Setting the DSCP value for IGMP messages

IPv4 uses an eight-bit ToS field to identify type of service for IP packets. As defined in RFC 2474, the first six bits contains the DSCP priority for prioritizing traffic in the network and the last two bits are reserved.

This configuration applies to only the IGMP messages that the local switch generates when the switch or its port acts as a member host, rather than those forwarded ones.

To set the DSCP value for IGMP messages:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IGMP-snooping view.	igmp-snooping	N/A
3. Set the DSCP value for IGMP messages.	dscp <i>dscp-value</i>	By default, the DSCP value in IGMP messages is 48.

Displaying and maintaining IGMP snooping

Task	Command	Remarks
Display IGMP snooping group information.	display igmp-snooping group [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display information about the hosts tracked by IGMP snooping.	display igmp-snooping host vlan <i>vlan-id group group-address</i> [source <i>source-address</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display static multicast MAC address entries.	display mac-address [<i>mac-address</i> [vlan <i>vlan-id</i>] [multicast] [vlan <i>vlan-id</i>] [count]] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display statistics for the IGMP messages learned by IGMP snooping.	display igmp-snooping statistics [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

Task	Command	Remarks
Remove all the dynamic group entries of a specified IGMP snooping group or all IGMP snooping groups.	reset igmp-snooping group { <i>group-address</i> all } [vlan <i>vlan-id</i>]	Available in user view. This command works only on an IGMP snooping-enabled VLAN, but not in a VLAN with IGMP enabled on its VLAN interface. This command cannot remove the static group entries of IGMP snooping groups.
Clear statistics for the IGMP messages learned by IGMP snooping.	reset igmp-snooping statistics	Available in user view.

IGMP snooping configuration examples

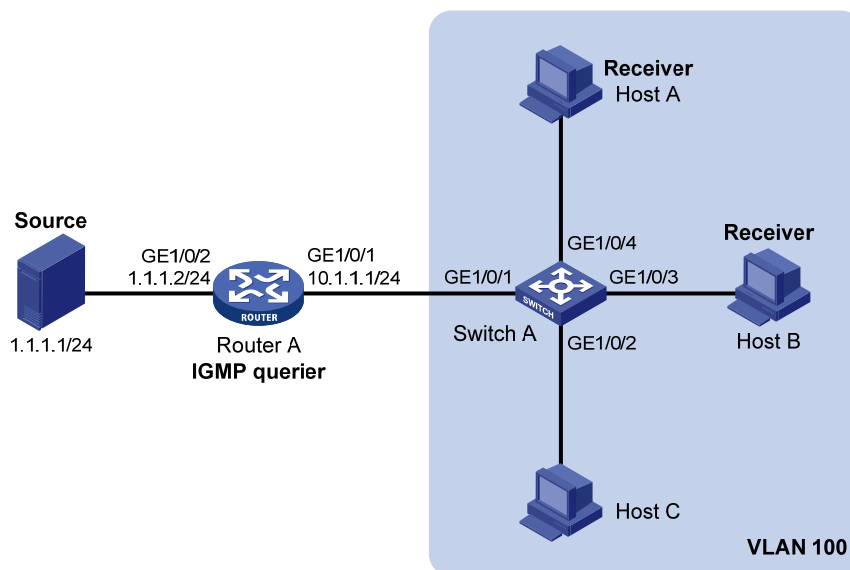
Group policy and simulated joining configuration example

Network requirements

As shown in [Figure 14](#), IGMPv2 runs on Router A, IGMPv2 snooping runs on Switch A, and Router A acts as the IGMP querier on the subnet.

The receivers, Host A and Host B, can receive multicast traffic addressed to multicast group 224.1.1.1 only. Multicast data for group 224.1.1.1 can be forwarded through GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 of Switch A even if Host A and Host B accidentally, temporarily stop receiving multicast data, and that Switch A drops unknown multicast data and does not broadcast the data to the VLAN where Switch A resides.

Figure 14 Network diagram



Configuration procedure

1. Configure an IP address and subnet mask for each interface as per [Figure 14](#). (Details not shown.)
2. On Router A, enable IP multicast routing, enable IGMP on GigabitEthernet 1/0/1, and enable PIM-DM on each interface.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

3. Configure Switch A:

Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN, and enable IGMP snooping and the function of dropping unknown multicast traffic in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping drop-unknown
[SwitchA-vlan100] quit
```

Configure a multicast group filter so that the hosts in VLAN 100 can join only the multicast group 224.1.1.1.

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 224.1.1.1 0
[SwitchA-acl-basic-2001] quit
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] group-policy 2001 vlan 100
[SwitchA-igmp-snooping] quit
```

Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 as simulated hosts for multicast group 224.1.1.1.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/4] quit
```

Verifying the configuration

Display detailed IGMP snooping group information in VLAN 100 on Switch A.

```
[SwitchA] display igmp-snooping group vlan 100 verbose
```

```

Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port.
    GE1/0/1                (D) ( 00:01:30 )
IP group(s):the following ip group(s) match to one mac group.
IP group address:224.1.1.1
(0.0.0.0, 224.1.1.1):
Attribute:    Host Port
Host port(s):total 2 port.
    GE1/0/3                (D) ( 00:03:23 )
    GE1/0/4                (D) ( 00:04:10 )
MAC group(s):
MAC group address:0100-5e01-0101
Host port(s):total 2 port.
    GE1/0/3
    GE1/0/4

```

The output shows that GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 of Switch A has joined multicast group 224.1.1.1.

Static port configuration example

Network requirements

As shown in [Figure 15](#), IGMPv2 runs on Router A, and IGMPv2 snooping runs on Switch A, Switch B, and Switch C. Router A acts as the IGMP querier.

Host A and host C are permanent receivers of multicast group 224.1.1.1. GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 on Switch C are required to be configured as static member ports for multicast group 224.1.1.1 to enhance the reliability of multicast traffic transmission.

Suppose STP runs on the network. To avoid data loops, the forwarding path from Switch A to Switch C is blocked under normal conditions, and multicast traffic flows to the receivers attached to Switch C only along the path of Switch A—Switch B—Switch C.

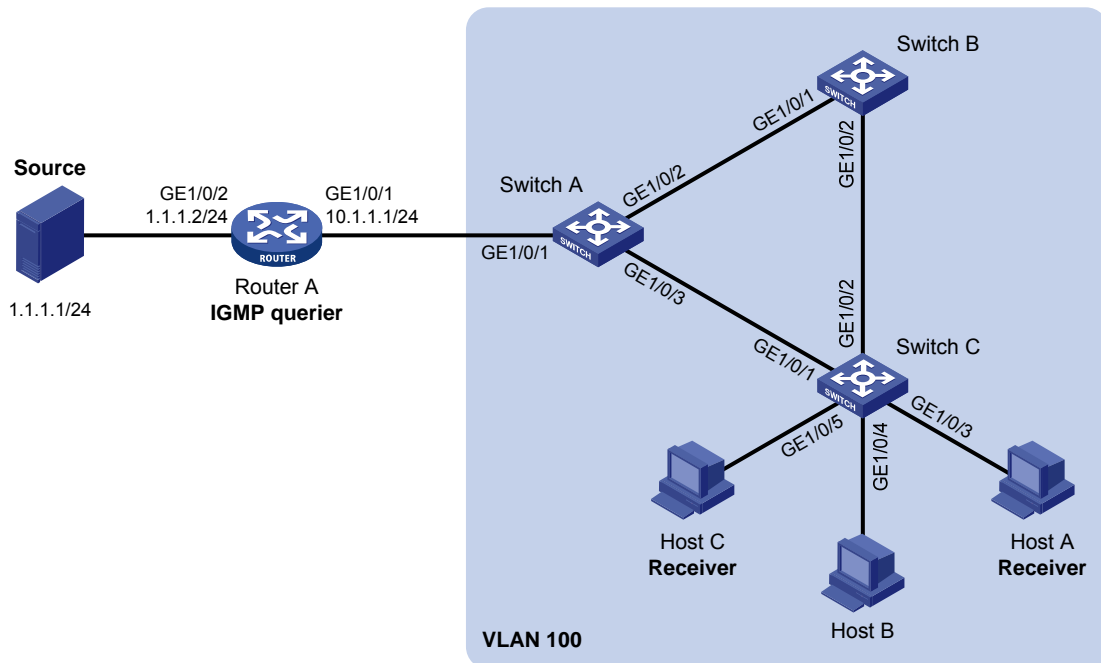
Configure GigabitEthernet 1/0/3 on Switch A as a static router port, so that multicast traffic can flow to the receivers nearly uninterruptedly along the path of Switch A—Switch C in the case that the path of Switch A—Switch B—Switch C gets blocked.

For more information about the Spanning Tree Protocol (STP), see *Layer 2—LAN Switching Configuration Guide*.

NOTE:

If no static router port is configured, when the path of Switch A—Switch B—Switch C gets blocked, at least one IGMP query-response cycle must be completed before the multicast data can flow to the receivers along the new path of Switch A—Switch C. Namely multicast delivery will be interrupted during this process.

Figure 15 Network diagram



Configuration procedure

1. Configure an IP address and subnet mask for each interface as per Figure 15. (Details not shown.)
2. On Router A, enable IP multicast routing, enable IGMP on GigabitEthernet 1/0/1, and enable PIM-DM on each interface.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

3. Configure Switch A:

Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to this VLAN, and enable IGMP snooping in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
```

Configure GigabitEthernet 1/0/3 to be a static router port.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

4. Configure Switch B:

Enable IGMP snooping globally.

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

Create VLAN 100, assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to this VLAN, and enable IGMP snooping in the VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

5. Configure Switch C:

Enable IGMP snooping globally.

```
<SwitchC> system-view
[SwitchC] igmp-snooping
[SwitchC-igmp-snooping] quit
```

Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to this VLAN, and enable IGMP snooping in the VLAN.

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] quit
```

Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 as static member ports for multicast group 224.1.1.1.

```
[SwitchC] interface GigabitEthernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
[SwitchC] interface GigabitEthernet 1/0/5
[SwitchC-GigabitEthernet1/0/5] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet1/0/5] quit
```

Verifying the configuration

Display detailed IGMP snooping group information in VLAN 100 on Switch A.

```
[SwitchA] display igmp-snooping group vlan 100 verbose
```

```

Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 2 port.
    GE1/0/1          (D) ( 00:01:30 )
    GE1/0/3          (S)
  IP group(s):the following ip group(s) match to one mac group.
  IP group address:224.1.1.1
  (0.0.0.0, 224.1.1.1):
  Attribute:      Host Port
  Host port(s):total 1 port.
    GE1/0/2          (D) ( 00:03:23 )
  MAC group(s):
  MAC group address:0100-5e01-0101
  Host port(s):total 1 port.
    GE1/0/2

```

The output shows that GigabitEthernet 1/0/3 of Switch A has become a static router port.

Display detailed IGMP snooping group information in VLAN 100 on Switch C.

```

[SwitchC] display igmp-snooping group vlan 100 verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 1 port.
    GE1/0/2          (D) ( 00:01:23 )
  IP group(s):the following ip group(s) match to one mac group.
  IP group address:224.1.1.1
  (0.0.0.0, 224.1.1.1):
  Attribute:      Host Port
  Host port(s):total 2 port.
    GE1/0/3          (S)
    GE1/0/5          (S)
  MAC group(s):
  MAC group address:0100-5e01-0101

```

```
Host port(s):total 2 port.  
GE1/0/3  
GE1/0/5
```

The output shows that GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 on Switch C have become static member ports for multicast group 224.1.1.1.

IGMP snooping querier configuration example

Network requirements

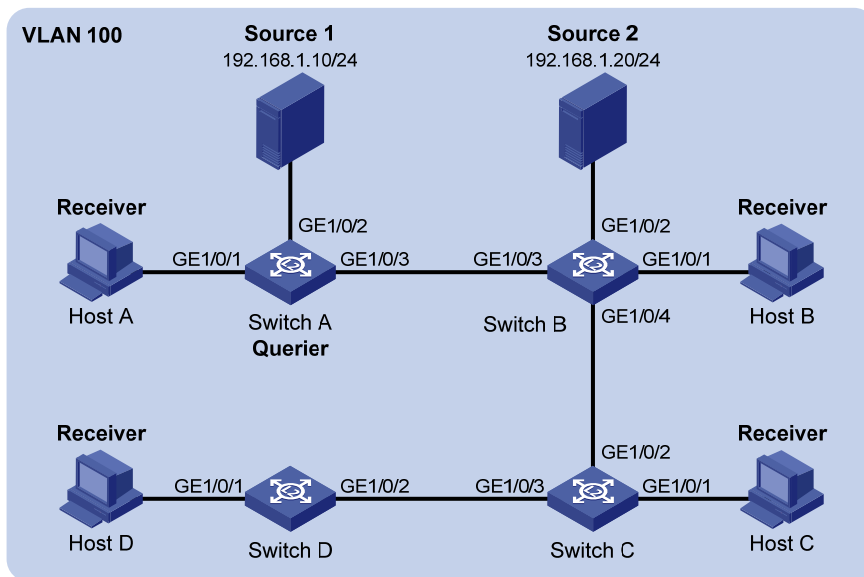
As shown in Figure 16, in a Layer 2-only network environment, two multicast sources Source 1 and Source 2 send multicast data to multicast groups 224.1.1.1 and 225.1.1.1 respectively, Host A and Host C are receivers of multicast group 224.1.1.1, and Host B and Host D are receivers of multicast group 225.1.1.1.

All the receivers run IGMPv2, and all the switches run IGMPv2 snooping. Switch A, which is close to the multicast sources, is chosen as the IGMP snooping querier.

To prevent flooding of unknown multicast traffic within the VLAN, be sure to configure all the switches to drop unknown multicast data packets.

Because a switch does not enlist a port that has heard an IGMP query with a source IP address of 0.0.0.0 (default) as a dynamic router port, configure a non-all-zero IP address as the source IP address of IGMP queries to ensure normal creation of Layer 2 multicast forwarding entries.

Figure 16 Network diagram



Configuration procedure

1. Configure switch A:
Enable IGMP snooping globally.
<SwitchA> system-view

```

[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
# Create VLAN 100 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to the
VLAN.
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
# Enable IGMP snooping and the function of dropping unknown multicast traffic in VLAN 100.
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping drop-unknown
# Enable the IGMP snooping querier function in VLAN 100
[SwitchA-vlan100] igmp-snooping querier
# Set the source IP address of IGMP general queries and group-specific queries to 192.168.1.1
in VLAN 100.
[SwitchA-vlan100] igmp-snooping general-query source-ip 192.168.1.1
[SwitchA-vlan100] igmp-snooping special-query source-ip 192.168.1.1
[SwitchA-vlan100] quit

```

2. Configure Switch B:

```

# Enable IGMP snooping globally.
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the
VLAN.
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
# Enable IGMP snooping and the function of dropping unknown multicast traffic in VLAN 100.
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] igmp-snooping drop-unknown
[SwitchB-vlan100] quit

```

Configurations on Switch C and Switch D are similar to the configuration on Switch B.

Verifying the configuration

After the IGMP snooping querier starts to work, all the switches but the querier can receive IGMP general queries. By using the **display igmp-snooping statistics** command, you can display statistics for the IGMP messages received. For example:

```

# Display IGMP message statistics on Switch B.
[SwitchB] display igmp-snooping statistics
Received IGMP general queries:3.
Received IGMPv1 reports:0.
Received IGMPv2 reports:12.
Received IGMP leaves:0.
Received IGMPv2 specific queries:0.
Sent IGMPv2 specific queries:0.
Received IGMPv3 reports:0.

```

```

Received IGMPv3 reports with right and wrong records:0.
Received IGMPv3 specific queries:0.
Received IGMPv3 specific sg queries:0.
Sent IGMPv3 specific queries:0.
Sent IGMPv3 specific sg queries:0.
Received error IGMP messages:0.

```

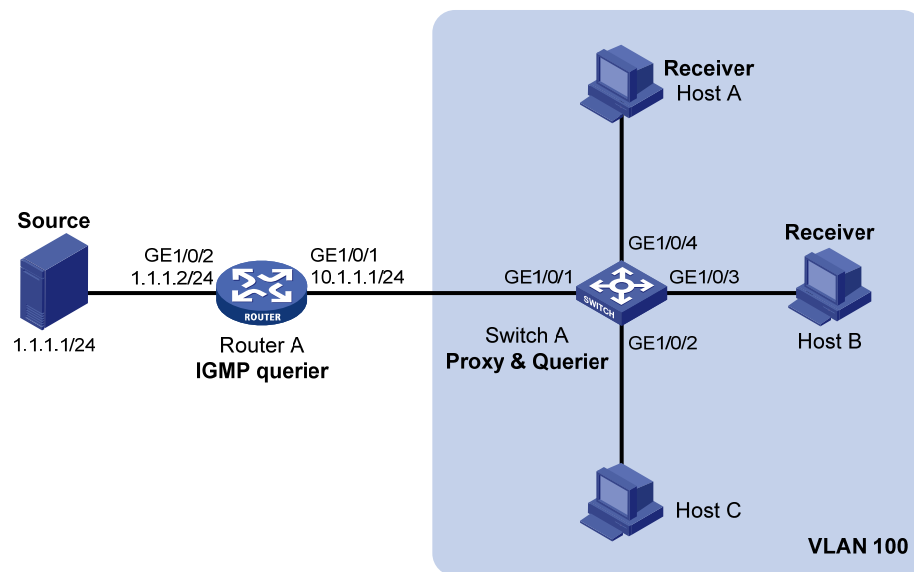
IGMP snooping proxying configuration example

Network requirements

As shown in [Figure 17](#), Router A runs IGMPv2 and Switch A runs IGMPv2 snooping. Router A acts as the IGMP querier.

Configure IGMP snooping proxying on Switch A, enabling the switch to forward IGMP reports and leave messages on behalf of attached hosts and to respond to IGMP queries from Router A and forward the queries to the hosts on behalf of Router A.

Figure 17 Network diagram



Configuration procedure

1. Configure an IP address and subnet mask for each interface as per [Figure 17](#). (Details not shown.)
2. On Router A, enable IP multicast routing, enable IGMP on GigabitEthernet 1/0/1, and enable PIM-DM on each interface.

```

<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2

```

```
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

3. Configure Switch A:

Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

Create VLAN 100, assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN, and enable IGMP snooping and IGMP snooping proxying in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping proxying enable
[SwitchA-vlan100] quit
```

Verifying the configuration

After the configuration is completed, Host A and Host B send IGMP join messages for group 224.1.1.1. Receiving the messages, Switch A sends a join message for the group out of port GigabitEthernet 1/0/1 (a router port) to Router A.

Use the **display igmp-snooping group** command and the **display igmp group** command to display information about IGMP snooping groups and IGMP multicast groups. For example:

Display information about IGMP snooping groups on Switch A.

```
[SwitchA] display igmp-snooping group
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
```

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port

Subvlan flags: R-Real VLAN, C-Copy VLAN

Vlan(id):100.

Total 1 IP Group(s).

Total 1 IP Source(s).

Total 1 MAC Group(s).

Router port(s):total 1 port.

GE1/0/1 (D) (00:01:23)

IP group(s):the following ip group(s) match to one mac group.

IP group address:224.1.1.1

(0.0.0.0, 224.1.1.1):

Host port(s):total 2 port.

GE1/0/3 (D)

GE1/0/4 (D)

MAC group(s):

MAC group address:0100-5e01-0101

Host port(s):total 2 port.

GE1/0/3

GE1/0/4

Display information about IGMP multicast groups on Router A.

```
[RouterA] display igmp group
Total 1 IGMP Group(s).
Interface group report information of VPN-Instance: public net
GigabitEthernet1/0/1(10.1.1.1):
  Total 1 IGMP Group reported
  Group Address      Last Reporter      Uptime      Expires
  224.1.1.1          0.0.0.0            00:00:06    00:02:04
```

When Host A leaves the multicast group, it sends an IGMP leave message to Switch A. Receiving the message, Switch A removes port GigabitEthernet 1/0/4 from the member port list of the forwarding entry for the group; however, it does not remove the group or forward the leave message to Router A because Host B is still in the group. Use the **display igmp-snooping group** command to display information about IGMP snooping groups. For example:

Display information about IGMP snooping groups on Switch A.

```
[SwitchA] display igmp-snooping group
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 1 port.
    GE1/0/1                (D) ( 00:01:23 )
  IP group(s):the following ip group(s) match to one mac group.
  IP group address:224.1.1.1
    (0.0.0.0, 224.1.1.1):
      Host port(s):total 1 port.
        GE1/0/3                (D)
  MAC group(s):
  MAC group address:0100-5e01-0101
  Host port(s):total 1 port.
    GE1/0/3
```

Multicast source and user control policy configuration example

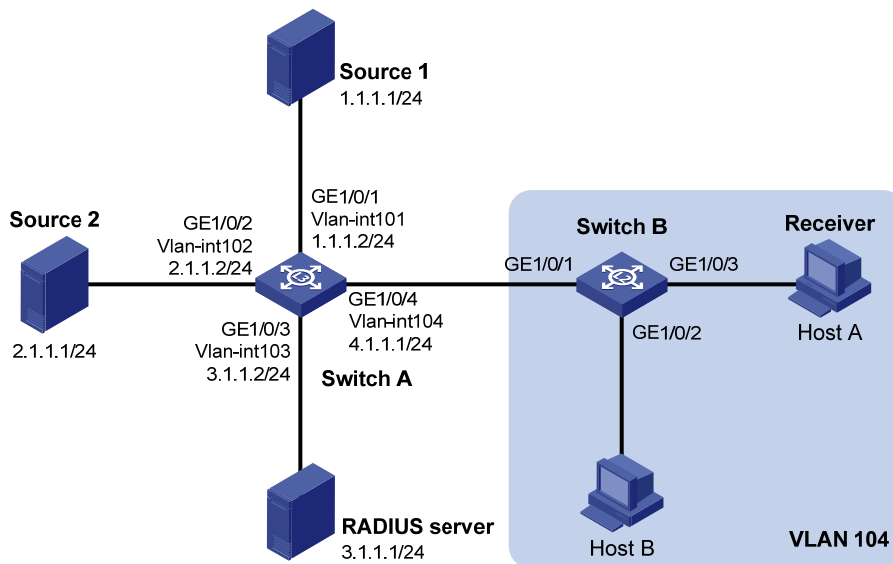
Network requirements

As shown in [Figure 18](#), Switch A is a Layer-3 switch. Switch A runs IGMPv2 and Switch B runs IGMPv2 snooping. Multicast sources and hosts run 802.1X client.

A multicast source control policy is configured on Switch A to block multicast flows from Source 2 to 224.1.1.1.

A multicast user control policy is configured on Switch B so that Host A can join or leave only multicast group 224.1.1.1.

Figure 18 Network diagram



Configuration procedures

1. Configure an IP address and subnet mask for each interface as per Figure 18. (Details not shown.)
2. Configure Switch A:

Create VLAN 101 through VLAN 104 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the four VLANs respectively.

```
<SwitchA> system-view
[SwitchA] vlan 101
[SwitchA-vlan101] port gigabitethernet 1/0/1
[SwitchA-vlan101] quit
[SwitchA] vlan 102
[SwitchA-vlan102] port gigabitethernet 1/0/2
[SwitchA-vlan102] quit
[SwitchA] vlan 103
[SwitchA-vlan103] port gigabitethernet 1/0/3
[SwitchA-vlan103] quit
[SwitchA] vlan 104
[SwitchA-vlan104] port gigabitethernet 1/0/4
[SwitchA-vlan104] quit
```

Enable IP multicast routing. Enable PIM-DM on VLAN-interface 101, VLAN-interface 102 and VLAN-interface 104, and enable IGMP on VLAN-interface 104.

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim dm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
```

```
[SwitchA-Vlan-interface102] pim dm
[SwitchA-Vlan-interface102] quit
[SwitchA] interface vlan-interface 104
[SwitchA-Vlan-interface104] pim dm
[SwitchA-Vlan-interface104] igmp enable
[SwitchA-Vlan-interface104] quit
```

Create QoS policy **policy1** to block multicast flows from Source 2 to 224.1.1.1.

```
[SwitchA] acl number 3001
[SwitchA-acl-adv-3001] rule permit udp source 2.1.1.1 0 destination 224.1.1.1 0
[SwitchA-acl-adv-3001] quit [SwitchA] traffic classifier classifier1
[SwitchA-classifier-classifier1] if-match acl 3001
[SwitchA-classifier-classifier1] quit
[SwitchA] traffic behavior behavior1
[SwitchA-behavior-behavior1] filter deny
[SwitchA-behavior-behavior1] quit
[SwitchA] qos policy policy1
[SwitchA-qospolicy-policy1] classifier classifier1 behavior behavior1
[SwitchA-qospolicy-policy1] quit
```

Create user profile **profile1**, apply QoS policy **policy1** to the inbound direction in user profile view, and enable the user profile.

```
[SwitchA] user-profile profile1
[SwitchA-user-profile-profile1] qos apply policy policy1 inbound
[SwitchA-user-profile-profile1] quit
[SwitchA] user-profile profile1 enable
```

Create RADIUS scheme **scheme1**; set the service type for the RADIUS server to **extended**; specify the IP addresses of the primary authentication/authorization server and accounting server as 3.1.1.1; set the shared keys to 123321; specify that no domain name is carried in a username sent to the RADIUS server.

```
[SwitchA] radius scheme scheme1
[SwitchA-radius-scheme1] server-type extended
[SwitchA-radius-scheme1] primary authentication 3.1.1.1
[SwitchA-radius-scheme1] key authentication 123321
[SwitchA-radius-scheme1] primary accounting 3.1.1.1
[SwitchA-radius-scheme1] key accounting 123321
[SwitchA-radius-scheme1] user-name-format without-domain
[SwitchA-radius-scheme1] quit
```

Create ISP domain **domain1**; reference **scheme1** for the authentication, authorization, and accounting of LAN users; specify **domain1** as the default ISP domain.

```
[SwitchA] domain domain1
[SwitchA-isp-domian1] authentication lan-access radius-scheme scheme1
[SwitchA-isp-domian1] authorization lan-access radius-scheme scheme1
[SwitchA-isp-domian1] accounting lan-access radius-scheme scheme1
[SwitchA-isp-domian1] quit
[SwitchA] domain default enable domain1
```

Globally enable 802.1X and then enable it on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 respectively.

```
[SwitchA] dot1x
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] dot1x
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] dot1x
[SwitchA-GigabitEthernet1/0/2] quit
```

3. Configure Switch B:

Globally enable IGMP snooping.

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

Create VLAN 104, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to this VLAN, and enable IGMP snooping in this VLAN.

```
[SwitchB] vlan 104
[SwitchB-vlan104] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[SwitchB-vlan104] igmp-snooping enable
[SwitchB-vlan104] quit
```

Create a user profile **profile2** to allow users to join or leave only one multicast group, 224.1.1.1. Then, enable the user profile.

```
[SwitchB] acl number 2001
[SwitchB-acl-basic-2001] rule permit source 224.1.1.1 0
[SwitchB-acl-basic-2001] quit
[SwitchB] user-profile profile2
[SwitchB-user-profile-profile2] igmp-snooping access-policy 2001
[SwitchB-user-profile-profile2] quit
[SwitchB] user-profile profile2 enable
```

Create a RADIUS scheme **scheme2**; set the service type for the RADIUS server to **extended**; specify the IP addresses of the primary authentication/authorization server and accounting server as 3.1.1.1; set the shared keys to 321123; specify that a username sent to the RADIUS server carry no domain name.

```
[SwitchB] radius scheme scheme2
[SwitchB-radius-scheme2] server-type extended
[SwitchB-radius-scheme2] primary authentication 3.1.1.1
[SwitchB-radius-scheme2] key authentication 321123
[SwitchB-radius-scheme2] primary accounting 3.1.1.1
[SwitchB-radius-scheme2] key accounting 321123
[SwitchB-radius-scheme2] user-name-format without-domain
[SwitchB-radius-scheme2] quit
```

Create an ISP domain **domain2**; reference **scheme2** for the authentication, authorization, and accounting of LAN users; specify **domain2** as the default ISP domain.

```
[SwitchB] domain domain2
[SwitchB-isp-domain2] authentication lan-access radius-scheme scheme2
[SwitchB-isp-domain2] authorization lan-access radius-scheme scheme2
[SwitchB-isp-domain2] accounting lan-access radius-scheme scheme2
```

```
[SwitchB-isp-domian2] quit
[SwitchB] domain default enable domain2
# Globally enable 802.1X and then enable it on GigabitEthernet 1/0/2 and GigabitEthernet
1/0/3 respectively.
[SwitchB] dot1x
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] dot1x
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] dot1x
[SwitchB-GigabitEthernet1/0/3] quit
```

4. Configure the RADIUS server:

On the RADIUS server, configure the parameters related to Switch A and Switch B. For more information, see the configuration guide of the RADIUS server.

Verifying the configuration

After the configurations, the two multicast sources and hosts initiate 802.1X authentication. After passing authentication, Source 1 sends multicast flows to 224.1.1.1 and Source 2 sends multicast flows to 224.1.1.2; Host A sends messages to join multicast groups 224.1.1.1 and 224.1.1.2. Use the **display igmp-snooping group** command to display information about IGMP snooping groups. For example:

Display information about IGMP snooping groups in VLAN 104 on Switch B.

```
[SwitchB] display igmp-snooping group vlan 104 verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):104.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port.
    GE1/0/1                (D) ( 00:01:30 )
IP group(s):the following ip group(s) match to one mac group.
  IP group address:224.1.1.1
    (0.0.0.0, 224.1.1.1):
      Attribute:    Host Port
      Host port(s):total 1 port.
        GE1/0/3                (D) ( 00:04:10 )
MAC group(s):
  MAC group address:0100-5e01-0101
  Host port(s):total 1 port.
    GE1/0/3
```

The output shows that GigabitEthernet 1/0/3 on Switch B has joined 224.1.1.1 but not 224.1.1.2.

Assume that Source 2 starts sending multicast traffic to 224.1.1.1. Use the **display multicast forwarding-table** to display the multicast forwarding table information.

Display information about 224.1.1.1 in the multicast forwarding table on Switch A.

```
[SwitchA] display multicast forwarding-table 224.1.1.1
Multicast Forwarding Table of VPN-Instance: public net
```

```
Total 1 entry
```

```
Total 1 entry matched
```

```
00001. (1.1.1.1, 224.1.1.1)
  MID: 0, Flags: 0x0:0
  Uptime: 00:08:32, Timeout in: 00:03:26
  Incoming interface: Vlan-interface101
  List of 1 outgoing interfaces:
    1: Vlan-interface104
  Matched 19648 packets(20512512 bytes), Wrong If 0 packets
  Forwarded 19648 packets(20512512 bytes)
```

The output shows that Switch A maintains a multicast forwarding entry for multicast packets from Source 1 to 224.1.1.1. No forwarding entry exists for packets from Source 2 to 224.1.1.1, which indicates that multicast packets from Source 2 are blocked.

Troubleshooting IGMP snooping

Layer 2 multicast forwarding cannot function

Symptom

Layer 2 multicast forwarding cannot function.

Analysis

IGMP snooping is not enabled.

Solution

1. Use the **display current-configuration** command to check the running status of IGMP snooping.
2. If IGMP snooping is not enabled, use the **igmp-snooping** command to enable IGMP snooping globally, and then use the **igmp-snooping enable** command to enable IGMP snooping in VLAN view.
3. If IGMP snooping is disabled only for the corresponding VLAN, use the **igmp-snooping enable** command in VLAN view to enable IGMP snooping in the corresponding VLAN.

Configured multicast group policy fails to take effect

Symptom

Although a multicast group policy has been configured to allow hosts to join specific multicast groups, the hosts can still receive multicast data addressed to other multicast groups.

Analysis

- The ACL rule is incorrectly configured.
- The multicast group policy is not correctly applied.
- The function of dropping unknown multicast data is not enabled, so unknown multicast data is flooded.

Solution

1. Use the **display acl** command to check the configured ACL rule. Make sure that the ACL rule conforms to the multicast group policy to be implemented.
2. Use the **display this** command in IGMP-snooping view or in the corresponding interface view to verify that the correct multicast group policy has been applied. If not, use the **group-policy** or **igmp-snooping group-policy** command to apply the correct multicast group policy.
3. Use the **display current-configuration** command to verify that the function of dropping unknown multicast data is enabled. If not, use the **igmp-snooping drop-unknown** command to enable the function of dropping unknown multicast data.

Appendix

Processing of multicast protocol messages

With Layer 3 multicast routing enabled, an IGMP snooping-enabled switch processes multicast protocol messages differently under different conditions, as follows:

1. If only IGMP is enabled on the switch, or if both IGMP and PIM are enabled on the switch, the switch does the following:
 - Maintains dynamic member ports or dynamic router ports according to IGMP packets
 - Maintains dynamic router ports according to PIM hello packets
2. If only PIM is enabled on the switch, the following occur:
 - The switch broadcasts IGMP messages as unknown messages in the VLAN.
 - After receiving a PIM hello message, the switch maintains the corresponding dynamic router port.
3. If IGMP is disabled on the switch, one of the following occurs:
 - If PIM is disabled, the switch deletes all its dynamic member ports and dynamic router ports.

- If PIM is enabled, the switch deletes only its dynamic member ports but not its dynamic router ports.

NOTE:

On a switch with Layer-3 multicast routing enabled, use the **display igmp group port-info** command to display Layer-2 port information.

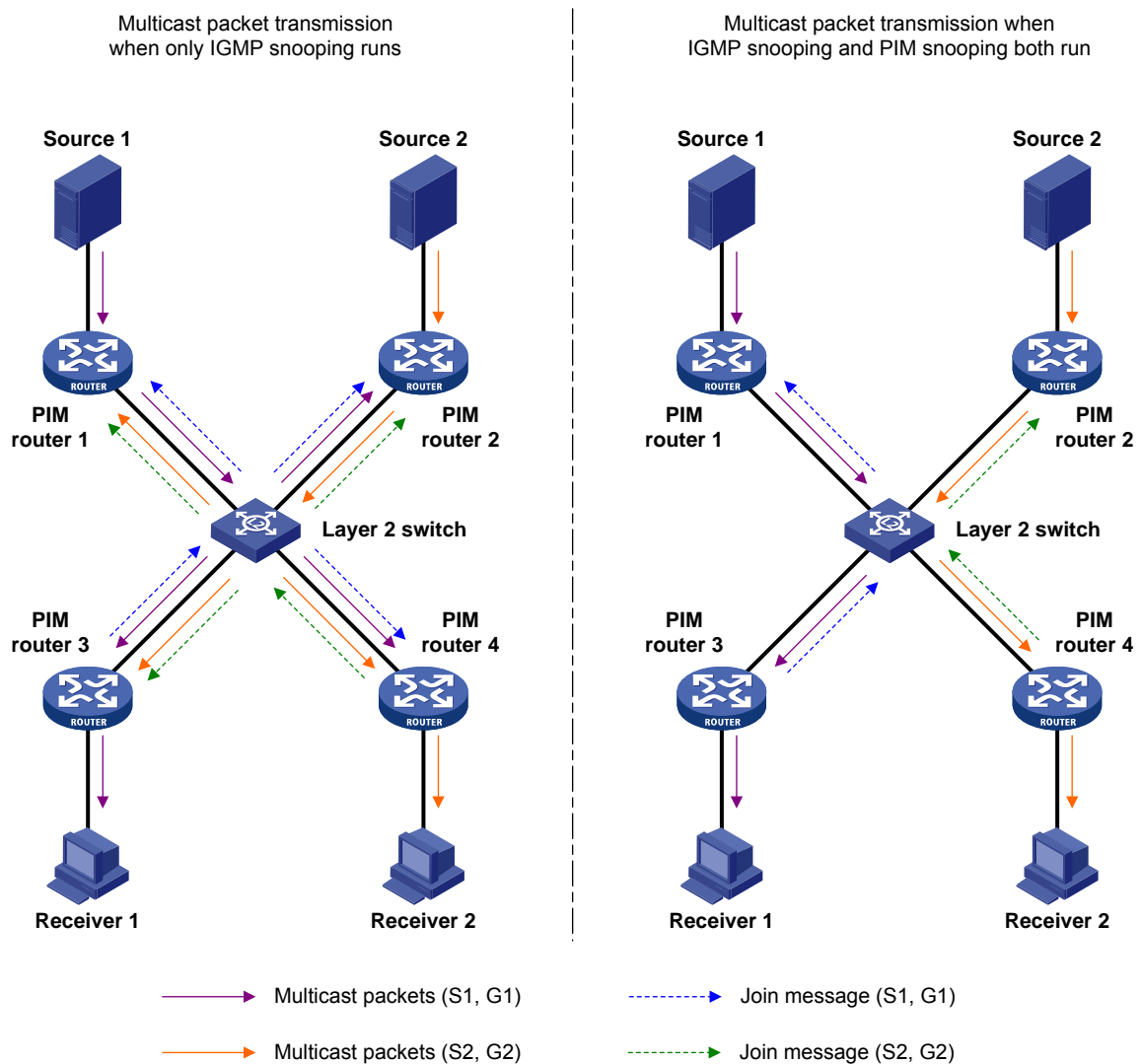
4. If PIM is disabled on the switch, one of the following occurs:
 - If IGMP is disabled, the switch deletes all its dynamic router ports.
 - If IGMP is enabled, the switch maintains all its dynamic member ports and dynamic router ports.

Configuring PIM snooping

Overview

Protocol Independent Multicast (PIM) snooping runs on Layer 2 devices. It determines which ports are interested in multicast data by analyzing the received PIM messages, and adds the ports to a multicast forwarding entry to make sure that multicast data can be forwarded to only the ports that are interested in the data.

Figure 19 Multicast packet transmission without or with PIM snooping



As shown in Figure 19, Source 1 sends multicast data to multicast group G1, and Source 2 sends multicast data to multicast group G2. Receiver 1 belongs to G1, and Receiver 2 belongs to G2. The Layer 2 switch's interfaces that connect to the PIM-capable routers are in the same VLAN.

- When the Layer 2 switch runs only IGMP snooping, it maintains the router ports according to the received PIM hello messages that PIM-capable routers send, broadcasts all other types of received PIM messages in the VLAN, and forwards all multicast data to all router ports in the VLAN. Each PIM-capable router in the VLAN, whether interested in the multicast data or not, can receive all multicast data and all PIM messages except PIM hello messages.
- When the Layer 2 switch runs both IGMP snooping and PIM snooping, it determines whether PIM-capable routers are interested in the multicast data addressed to a multicast group according to PIM messages received from the routers, and adds only the ports for connecting the routers that are interested in the data to a multicast forwarding entry. Then, the Layer 2 switch forwards PIM messages and multicast data to only the routers that are interested in the data, saving network bandwidth.

For more information about IGMP snooping and the router port, see "[Configuring IGMP snooping](#)."

For more information about PIM, see "[Configuring PIM \(available only on the HP 5500 EI\)](#)."

Configuring PIM snooping

When you configure PIM snooping, follow these guidelines:

- Before configuring PIM snooping for a VLAN, be sure to enable IGMP snooping globally and specifically for the VLAN.
- After you enable PIM snooping in a VLAN, PIM snooping works only on the member interfaces of the VLAN.
- PIM snooping does not work in the sub-VLANs of a multicast VLAN. For more information about multicast VLAN, see "[Configuring multicast VLANs](#)."
- In a network with PIM snooping enabled switches, configure the size of each join/prune message no more than the path maximum transmission unit (MTU) on the PIM-enabled edge router on the receiver side. For more information about the join/prune messages, see "[Configuring PIM \(available only on the HP 5500 EI\)](#)."

To configure PIM snooping:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IGMP snooping globally and enter IGMP-snooping view.	igmp-snooping	Disabled by default
3. Return to system view.	quit	N/A
4. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
5. Enable IGMP snooping in the VLAN.	igmp-snooping enable	Disabled by default
6. Enable PIM snooping in the VLAN.	pim-snooping enable	Disabled by default

For more information about the **igmp-snooping** and **igmp-snooping enable** commands, see *IP Multicast Command Reference*.

Displaying and maintaining PIM snooping

Task	Command	Remarks
Display PIM snooping neighbor information.	display pim-snooping neighbor [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display PIM snooping routing entries.	display pim-snooping routing-table [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the statistics information of PIM messages learned by PIM snooping.	display pim-snooping statistics [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Clear the statistics information of PIM messages learned by PIM snooping.	reset pim-snooping statistics	Available in user view

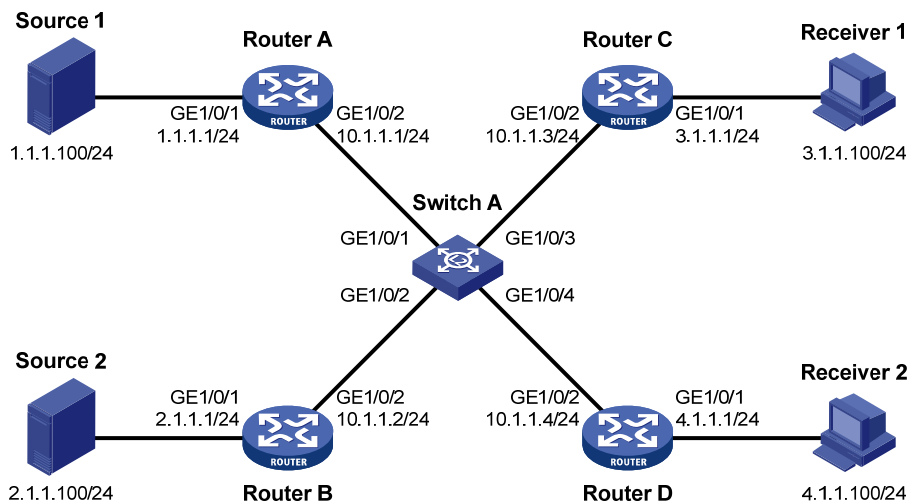
PIM snooping configuration example

Network requirements

As shown in [Figure 20](#), Source 1 sends multicast data to multicast group 224.1.1.1, and Source 2 sends multicast data to multicast group 225.1.1.1. Receiver 1 belongs to multicast group 224.1.1.1, and Receiver 2 belongs to multicast group 225.1.1.1. Router C and Router D run IGMP on their interface GigabitEthernet 1/0/1. Router A, Router B, Router C, and Router D run PIM-SM, and interface GigabitEthernet 1/0/2 on Router A acts as a C-BSR and C-RP.

Configure IGMP snooping and PIM snooping on Switch A so that Switch A forwards PIM messages and multicast data to only the routers that are interested in the multicast data.

Figure 20 Network diagram



Configuration procedure

1. Configure an IP address and subnet mask for each interface according to Figure 20. (Details not shown.)
2. On Router A, enable IP multicast routing, enable PIM-SM on each interface, and configure interface GigabitEthernet 1/0/2 as a C-BSR and C-RP.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim sm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim sm
[RouterA-GigabitEthernet1/0/2] quit
[RouterA] pim
[RouterA-pim] c-bsr gigabitethernet 1/0/2
[RouterA-pim] c-rp gigabitethernet 1/0/2
```

3. On Router B, enable IP multicast routing and enable PIM-SM on each interface.

```
<RouterB> system-view
[RouterB] multicast routing-enable
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] pim sm
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] pim sm
```

4. On Router C, enable IP multicast routing, enable PIM-SM on each interface, and enable IGMP on GigabitEthernet 1/0/1.

```
<RouterC> system-view
[RouterC] multicast routing-enable
[RouterC] interface gigabitethernet 1/0/1
```

```

[RouterC-GigabitEthernet1/0/1] pim sm
[RouterC-GigabitEthernet1/0/1] igmp enable
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] pim sm

```

5. Configure Router D in the same way as you configure Router C. (Details not shown.)

6. Configure Switch A:

Enable IGMP snooping globally.

```

<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit

```

Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN, and enable IGMP snooping and PIM snooping in the VLAN.

```

[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] pim-snooping enable
[SwitchA-vlan100] quit

```

Verifying the configuration

On Switch A, display the PIM snooping neighbor information of VLAN 100.

```

[SwitchA] display pim-snooping neighbor vlan 100
Total number of neighbors: 4

```

VLAN ID: 100

Total number of neighbors: 4

Neighbor	Port	Expires	Option Flags
10.1.1.1	GE1/0/1	02:02:23	LAN Prune Delay
10.1.1.2	GE1/0/2	03:00:05	LAN Prune Delay
10.1.1.3	GE1/0/3	02:22:13	LAN Prune Delay
10.1.1.4	GE1/0/4	03:07:22	LAN Prune Delay

The output shows that Router A, Router B, Router C, and Router D are PIM snooping neighbors.

On Switch A, display the PIM snooping routing information of VLAN 100.

```

[SwitchA] display pim-snooping routing-table vlan 100 slot 1
Total 2 entry(ies)
FSM Flag: NI-no info, J-join, PP-prune pending

```

VLAN ID: 100

Total 2 entry(ies)

(* , 224.1.1.1)

Upstream neighbor: 10.1.1.1

Upstream port: GE1/0/1

Total number of downstream ports: 1

1: GE1/0/3

Expires: 00:03:01, FSM: J

(* , 225.1.1.1)

```
Upstream neighbor: 10.1.1.2
Upstream port: GE1/0/2
Total number of downstream ports: 1
  1: GE1/0/4
Expires: 00:01:05, FSM: J
```

The output shows that Switch A will forward the multicast data intended for multicast group 224.1.1.1 to only Router C, and forward the multicast data intended for multicast group 225.1.1.1 to only Router D.

Troubleshooting PIM snooping

PIM snooping does not work

Symptom

PIM snooping does not work on the switch.

Analysis

IGMP snooping or PIM snooping is not enabled on the switch.

Solution

1. Use the **display current-configuration** command to check the status of IGMP snooping and PIM snooping.
2. If IGMP snooping is not enabled, enter system view and use the **igmp-snooping** command to enable IGMP snooping globally. Then, enter VLAN view and use the **igmp-snooping enable** and **pim-snooping enable** commands to enable IGMP snooping and PIM snooping in the VLAN.
3. If PIM snooping is not enabled, enter VLAN view and use the **pim-snooping enable** command to enable PIM snooping in the VLAN.

Some downstream PIM-capable routers cannot receive multicast data

Symptom

In a network with fragmented join/prune messages, some downstream PIM-capable routers cannot receive multicast data.

Analysis

PIM snooping cannot reassemble messages, and it cannot maintain the status of downstream routers that the join/prune message fragments carry. To ensure the normal operation of the system, PIM snooping must broadcast join/prune message fragments in the VLAN. However, if the VLAN has a PIM-capable router that has the join suppression function enabled, the broadcast join/prune message fragments might suppress the join messages of other PIM-capable routers in the VLAN. As a result, some PIM-capable routers cannot receive the multicast data destined for a specific multicast group because their join

messages are suppressed. To solve this problem, disable the join suppression function on all PIM-capable routers that connect to the PIM snooping-capable switch in the VLAN.

Solution

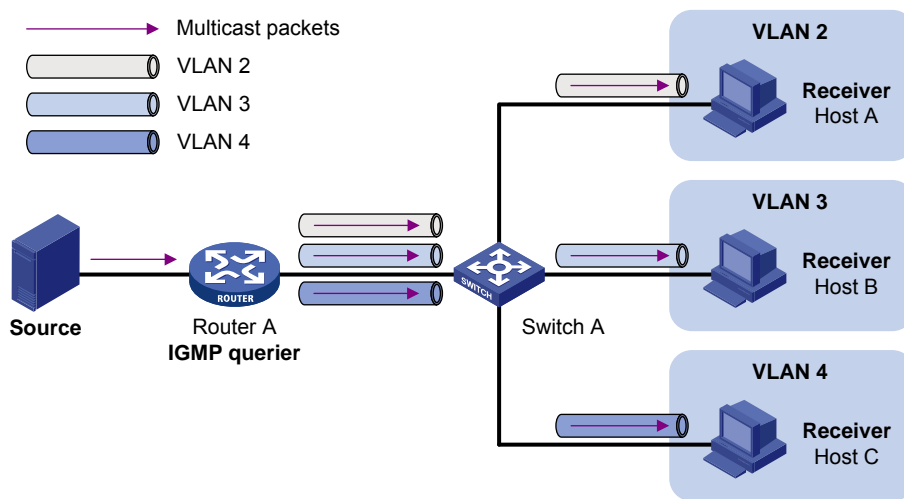
1. Use the **pim hello-option neighbor-tracking** command to enable the neighbor tracking function on the interfaces of PIM routers that connect to the PIM snooping-capable switch.
2. If a PIM-capable router cannot be enabled with the neighbor tracking function, you have to disable PIM snooping on the switch.

Configuring multicast VLANs

Overview

In the traditional multicast programs-on-demand mode shown in [Figure 21](#), when hosts (Host A, Host B and Host C) that belong to different VLANs require multicast programs-on-demand service, the Layer 3 device, Router A, must forward a separate copy of the multicast traffic in each user VLAN to the Layer 2 device, Switch A. This results in not only waste of network bandwidth but also extra burden on the Layer 3 device.

Figure 21 Multicast transmission without multicast VLAN



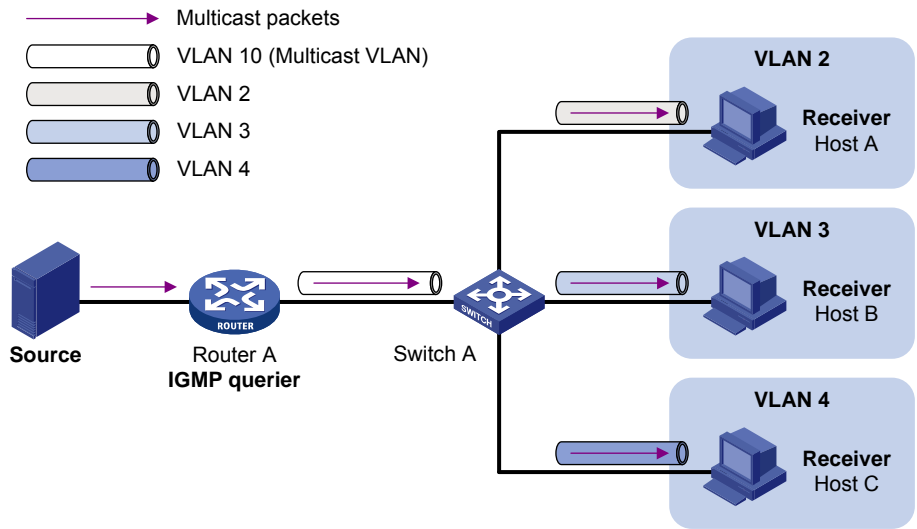
The multicast VLAN feature configured on the Layer 2 device is the solution to this issue. With the multicast VLAN feature, the Layer 3 device replicates the multicast traffic only in the multicast VLAN instead of making a separate copy of the multicast traffic in each user VLAN. This saves network bandwidth and lessens the burden on the Layer 3 device.

The multicast VLAN feature can be implemented in sub-VLAN-based multicast VLAN and port-based multicast VLAN.

Sub-VLAN-based multicast VLAN

As shown in [Figure 22](#), Host A, Host B, and Host C are in different user VLANs. On Switch A, configure VLAN 10 as a multicast VLAN, configure all the user VLANs as sub-VLANs of VLAN 10, and enable IGMP snooping in the multicast VLAN.

Figure 22 Sub-VLAN-based multicast VLAN

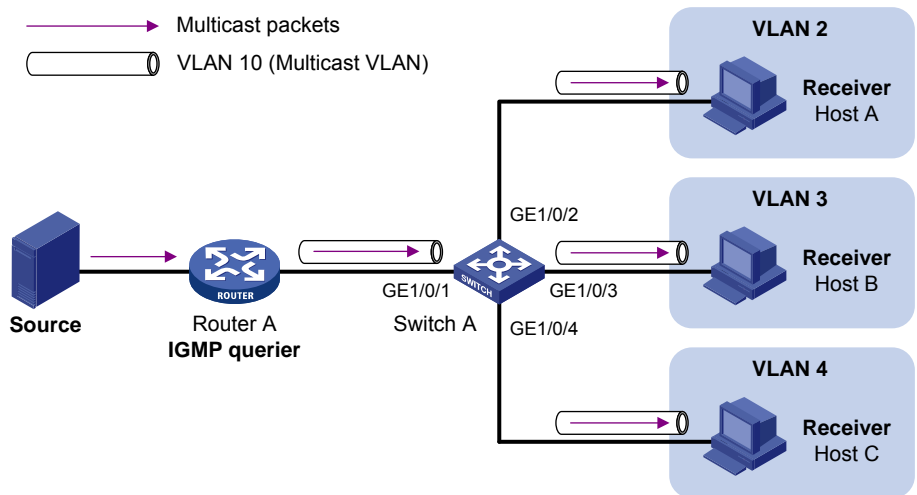


After the configuration, IGMP snooping manages router ports in the multicast VLAN and member ports in the sub-VLANs. When forwarding multicast data to Switch A, Router A sends only one copy of multicast data to Switch A in the multicast VLAN, and Switch A distributes the data to the multicast VLAN's sub-VLANs that contain receivers.

Port-based multicast VLAN

As shown in Figure 23, Host A, Host B, and Host C are in different user VLANs. All the user ports (ports with attached hosts) on Switch A are hybrid ports. On Switch A, configure VLAN 10 as a multicast VLAN, assign all the user ports to VLAN 10, and enable IGMP snooping in the multicast VLAN and all the user VLANs.

Figure 23 Port-based multicast VLAN



After the configuration, if Switch A receives an IGMP message on a user port, it tags the message with the multicast VLAN ID and relays it to the IGMP querier, so that IGMP snooping can uniformly manage the router port and member ports in the multicast VLAN. When Router A forwards multicast data to

Switch A, it sends only one copy of multicast data to Switch A in the multicast VLAN, and Switch A distributes the data to all the member ports in the multicast VLAN.

For more information about IGMP snooping, router ports, and member ports, see "[Configuring IGMP snooping](#)."

For more information about VLAN tags, see *Layer 2—LAN Switching Configuration Guide*.

Multicast VLAN configuration task list

Task	Remarks
Configuring a sub-VLAN-based multicast VLAN	Required
Configuring a port-based multicast VLAN	Configuring user port attributes Configuring multicast VLAN ports Use either approach.

NOTE:

If you have configured both sub-VLAN-based multicast VLAN and port-based multicast VLAN on a device, the port-based multicast VLAN configuration is given preference.

Configuring a sub-VLAN-based multicast VLAN

Before you configure sub-VLAN-based multicast VLAN, complete the following tasks:

- Create VLANs as required.
- Enable IGMP snooping in the VLAN to be configured as a multicast VLAN.

Configuration guidelines

- For the HP 5500 EI switches, you cannot configure multicast VLAN on a device with IP multicast routing enabled.
- The VLAN to be configured as a multicast VLAN must exist.
- The VLANs to be configured as sub-VLANs of the multicast VLAN must exist and must not be multicast VLANs or sub-VLANs of any other multicast VLAN.
- The total number of sub-VLANs of a multicast VLAN must not exceed the maximum number the system can support.

Configuration procedure

In this approach, you configure a VLAN as a multicast VLAN and configure user VLANs as sub-VLANs of the multicast VLAN.

To configure a sub-VLAN-based multicast VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the specified VLAN as a multicast VLAN and enter multicast VLAN view.	multicast-vlan <i>vlan-id</i>	By default, a VLAN is not a multicast VLAN.
3. Configure the specified VLANs as sub-VLANs of the multicast VLAN.	subvlan <i>vlan-list</i>	By default, a multicast VLAN has no sub-VLANs.

Configuring a port-based multicast VLAN

When you configure a port-based multicast VLAN, you must configure the attributes of each user port and then assign the ports to the multicast VLAN.

A user port can be configured as a multicast VLAN port only if it is an Ethernet port, or Layer 2 aggregate interface.

In Ethernet interface view or Layer 2 aggregate interface view, configurations that you make are effective on only the current port. In port group view, configurations that you make are effective on all ports in the current port group.

Configuration prerequisites

Before you configure a port-based multicast VLAN, complete the following tasks:

- Create VLANs as required.
- Enable IGMP snooping in the VLAN to be configured as a multicast VLAN.
- Enable IGMP snooping in all the user VLANs.

Configuring user port attributes

First, configure the user ports as hybrid ports that permit packets of the specified user VLAN to pass, and configure the user VLAN to which the user ports belong as the default VLAN.

Then, configure the user ports to permit packets of the multicast VLAN to pass and untag the packets. Thus, after receiving multicast packets tagged with the multicast VLAN ID from the upstream device, the Layer 2 device untags the multicast packets and forwards them to its downstream device.

To configure user port attributes:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter interface view or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
3. Configure the user port link type as hybrid.	port link-type hybrid	Access by default
4. Specify the user VLAN that comprises the current user ports as the default VLAN.	port hybrid pvid vlan <i>vlan-id</i>	VLAN 1 by default
5. Configure the current user ports to permit packets of the specified multicast VLANs to pass and untag the packets.	port hybrid vlan <i>vlan-id-list</i> untagged	By default, a hybrid port permits only packets of VLAN 1 to pass.

For more information about the **port link-type**, **port hybrid pvid vlan**, and **port hybrid vlan** commands, see *Layer 2—LAN Switching Command Reference*.

Configuring multicast VLAN ports

In this approach, you configure a VLAN as a multicast VLAN and assign user ports to it. You can do this by either adding the user ports in the multicast VLAN or specifying the multicast VLAN on the user ports. These two methods provide the same result.

Configuration guidelines

- For the HP 5500 EI switches, you cannot configure multicast VLAN on a device with multicast routing enabled.
- The VLAN to be configured as a multicast VLAN must exist.
- A port can belong to only one multicast VLAN.

Configuration procedure

To configure multicast VLAN ports in multicast VLAN view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the specified VLAN as a multicast VLAN and enter multicast VLAN view.	multicast-vlan <i>vlan-id</i>	By default, a VLAN is not a multicast VLAN.
3. Assign ports to the multicast VLAN.	port <i>interface-list</i>	By default, a multicast VLAN has no ports.

To configure multicast VLAN ports in interface view or port group view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the specified VLAN as a multicast VLAN and enter multicast VLAN view.	multicast-vlan <i>vlan-id</i>	By default, a VLAN is not a multicast VLAN.
3. Return to system view.	quit	N/A
4. Enter interface view or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
5. Configure the current port as a member port of the multicast VLAN.	port multicast-vlan <i>vlan-id</i>	By default, a user port does not belong to any multicast VLAN.

Displaying and maintaining multicast VLAN

Task	Command	Remarks
Display information about a multicast VLAN.	display multicast-vlan [<i>vlan-id</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view

Multicast VLAN configuration examples

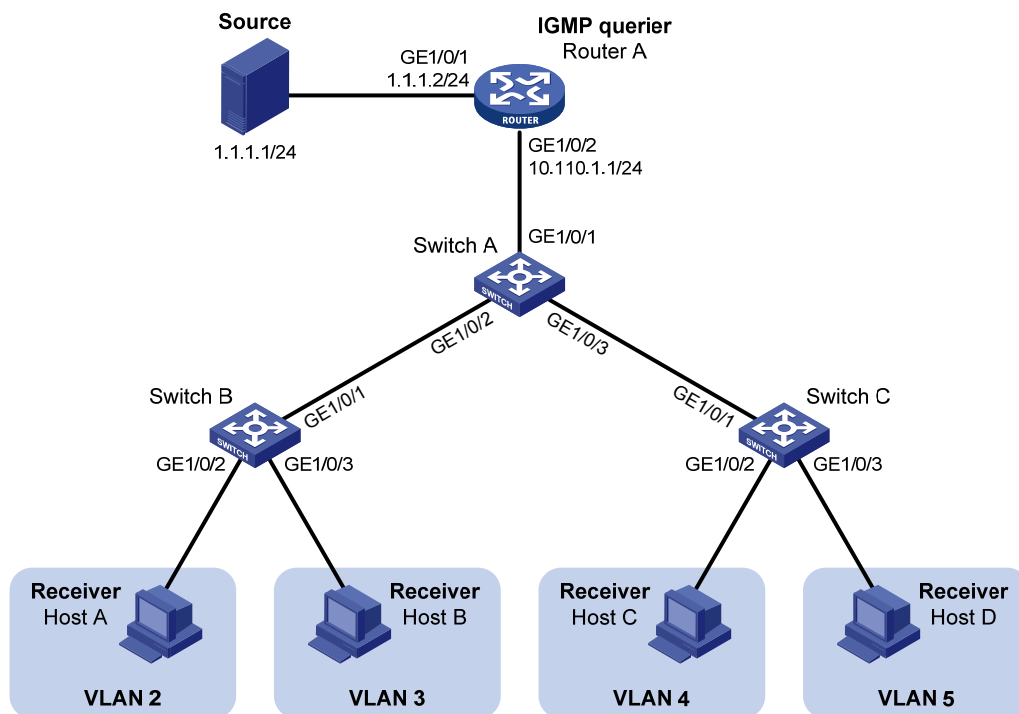
Sub-VLAN-based multicast VLAN configuration example

Network requirements

As shown in [Figure 24](#), IGMPv2 runs on Router A, and IGMPv2 snooping runs on Switch A, Switch B, and Switch C. Router A acts as the IGMP querier. The multicast source sends multicast data to multicast group 224.1.1.1. Host A, Host B, Host C, and Host D are receivers of the multicast group. The hosts belong to VLAN 2 through VLAN 5 respectively.

Configure the sub-VLAN-based multicast VLAN feature on Switch A so that Router A just sends multicast data to Switch A through the multicast VLAN and Switch A forwards the traffic to the receivers that belong to different user VLANs.

Figure 24 Network diagram



Configuration procedure

1. Configure an IP address and subnet mask for each interface as per Figure 24. (Details not shown.)
2. On Router A, enable IP multicast routing, enable PIM-DM on each interface and enable IGMP on the host-side interface GigabitEthernet 1/0/2.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] igmp enable
```

3. Configure Switch A:

Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

Create VLAN 2 through VLAN 5.

```
[SwitchA] vlan 2 to 5
```

Configure GigabitEthernet 1/0/2 as a trunk port, and assign it to VLAN 2 and VLAN 3.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 2 3
```

```
[SwitchA-GigabitEthernet1/0/2] quit
# Configure GigabitEthernet 1/0/3 as a trunk port, and assign it to VLAN 4 and VLAN 5.
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 4 5
[SwitchA-GigabitEthernet1/0/3] quit
# Create VLAN 10, assign GigabitEthernet 1/0/1 to this VLAN and enable IGMP snooping in the
VLAN.
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] igmp-snooping enable
[SwitchA-vlan10] quit
# Configure VLAN 10 as a multicast VLAN and configure VLAN 2 through VLAN 5 as its
sub-VLANs.
[SwitchA] multicast-vlan 10
[SwitchA-mvlan-10] subvlan 2 to 5
[SwitchA-mvlan-10] quit
```

4. Configure Switch B:

```
# Enable IGMP snooping globally.
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
# Create VLAN 2, assign GigabitEthernet 1/0/2 to VLAN 2, and enable IGMP snooping in the
VLAN.
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/2
[SwitchB-vlan2] igmp-snooping enable
[SwitchB-vlan2] quit
# Create VLAN 3, assign GigabitEthernet 1/0/3 to VLAN 3, and enable IGMP snooping in the
VLAN.
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3
[SwitchB-vlan3] igmp-snooping enable
[SwitchB-vlan3] quit
# Configure GigabitEthernet 1/0/1 as a trunk port, and assign it to VLAN 2 and VLAN 3.
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2 3
```

5. Configure Switch C in the same way as you configure Switch B. (Details not shown.)

Verifying the configuration

```
# Display information about the multicast VLAN.
[SwitchA] display multicast-vlan
Total 1 multicast-vlan(s)
```

```
Multicast vlan 10
  subvlan list:
    vlan 2-5
  port list:
    no port
```

Display the IGMP snooping multicast group information on Switch A.

```
[SwitchA] display igmp-snooping group
Total 5 IP Group(s).
Total 5 IP Source(s).
Total 5 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):2.
```

```
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
```

```
Router port(s):total 0 port(s).
```

```
IP group(s):the following ip group(s) match to one mac group.
```

```
IP group address:224.1.1.1
```

```
(0.0.0.0, 224.1.1.1):
```

```
Host port(s):total 1 port(s).
```

```
GE1/0/2 (D)
```

```
MAC group(s):
```

```
MAC group address:0100-5e01-0101
```

```
Host port(s):total 1 port(s).
```

```
GE1/0/2
```

```
Vlan(id):3.
```

```
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
```

```
Router port(s):total 0 port(s).
```

```
IP group(s):the following ip group(s) match to one mac group.
```

```
IP group address:224.1.1.1
```

```
(0.0.0.0, 224.1.1.1):
```

```
Host port(s):total 1 port(s).
```

```
GE1/0/2 (D)
```

```
MAC group(s):
```

```
MAC group address:0100-5e01-0101
```

```
Host port(s):total 1 port(s).
```

```
GE1/0/2
```

```
Vlan(id):4.
```

```
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
```

```

Router port(s):total 0 port(s).
IP group(s):the following ip group(s) match to one mac group.
  IP group address:224.1.1.1
    (0.0.0.0, 224.1.1.1):
      Host port(s):total 1 port(s).
        GE1/0/3                (D)
MAC group(s):
  MAC group address:0100-5e01-0101
  Host port(s):total 1 port(s).
    GE1/0/3

Vlan(id):5.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 0 port(s).
  IP group(s):the following ip group(s) match to one mac group.
    IP group address:224.1.1.1
      (0.0.0.0, 224.1.1.1):
        Host port(s):total 1 port(s).
          GE1/0/3                (D)
  MAC group(s):
    MAC group address:0100-5e01-0101
    Host port(s):total 1 port(s).
      GE1/0/3

Vlan(id):10.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 1 port(s).
    GE1/0/1                (D)
  IP group(s):the following ip group(s) match to one mac group.
    IP group address:224.1.1.1
      (0.0.0.0, 224.1.1.1):
        Host port(s):total 0 port(s).
  MAC group(s):
    MAC group address:0100-5e01-0101
    Host port(s):total 0 port(s).

```

The output shows that IGMP snooping is maintaining the router port in the multicast VLAN (VLAN 10) and the member ports in the sub-VLANs (VLAN 2 through VLAN 5).

Port-based multicast VLAN configuration example

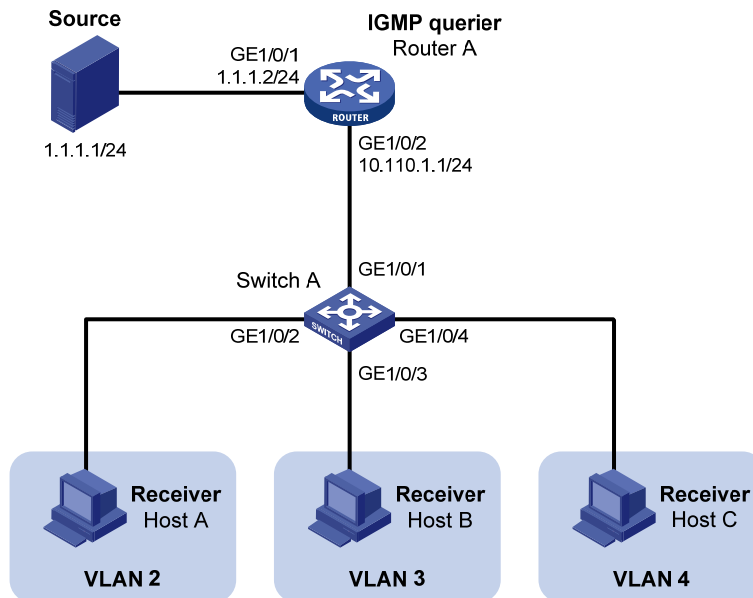
Network requirements

As shown in [Figure 25](#), IGMPv2 runs on Router A. IGMPv2 Snooping runs on Switch A. Router A acts as the IGMP querier. The multicast source sends multicast data to multicast group 224.1.1.1. Host A, Host B,

and Host C are receivers of the multicast group, and the hosts belong to VLAN 2 through VLAN 4 respectively.

Configure the port-based multicast VLAN feature on Switch A so that Router A just sends multicast data to Switch A through the multicast VLAN and Switch A forwards the multicast data to the receivers that belong to different user VLANs.

Figure 25 Network diagram



Configuration procedure

1. Configure the IP address and subnet mask for each interface as per Figure 25. (Details not shown.)
2. On Router A, enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on the host-side interface GigabitEthernet 1/0/2.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] igmp enable
```

3. Configure Switch A:

Enable IGMP snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

Create VLAN 10, assign GigabitEthernet 1/0/1 to VLAN 10, and enable IGMP snooping in this VLAN.

```
[SwitchA] vlan 10
```

```
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] igmp-snooping enable
[SwitchA-vlan10] quit
```

Create VLAN 2 and enable IGMP snooping in the VLAN.

```
[SwitchA] vlan 2
[SwitchA-vlan2] igmp-snooping enable
[SwitchA-vlan2] quit
```

The configuration for VLAN 3 and VLAN 4 is similar. (Details not shown.)

Configure GigabitEthernet 1/0/2 as a hybrid port. Configure VLAN 2 as the default VLAN. Configure GigabitEthernet 1/0/2 to permit packets of VLAN 2 and VLAN 10 to pass and untag the packets when forwarding them.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type hybrid
[SwitchA-GigabitEthernet1/0/2] port hybrid pvid vlan 2
[SwitchA-GigabitEthernet1/0/2] port hybrid vlan 2 untagged
[SwitchA-GigabitEthernet1/0/2] port hybrid vlan 10 untagged
[SwitchA-GigabitEthernet1/0/2] quit
```

The configuration for GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 is similar. (Details not shown.)

Configure VLAN 10 as a multicast VLAN.

```
[SwitchA] multicast-vlan 10
```

Assign GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to VLAN 10.

```
[SwitchA-mvlan-10] port gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[SwitchA-mvlan-10] quit
```

Assign GigabitEthernet 1/0/4 to VLAN 10.

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port multicast-vlan 10
[SwitchA-GigabitEthernet1/0/4] quit
```

Verifying the configuration

Display the multicast VLAN information on Switch A.

```
[SwitchA] display multicast-vlan
Total 1 multicast-vlan(s)

Multicast vlan 10
  subvlan list:
    no subvlan
  port list:
    GE1/0/2                GE1/0/3                GE1/0/4
```

Display the IGMP snooping multicast group information on Switch A.

```
[SwitchA] display igmp-snooping group
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):10.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 1 port(s).
    GE1/0/1                (D)
  IP group(s):the following ip group(s) match to one mac group.
  IP group address:224.1.1.1
  (0.0.0.0, 224.1.1.1):
    Host port(s):total 3 port(s).
      GE1/0/2                (D)
      GE1/0/3                (D)
      GE1/0/4                (D)
  MAC group(s):
  MAC group address:0100-5e01-0101
  Host port(s):total 3 port(s).
    GE1/0/2
    GE1/0/3
    GE1/0/4
```

The output shows that IGMP snooping is maintaining the router ports and member ports in VLAN 10.

Configuring multicast routing and forwarding (available only on the HP 5500 EI)

Overview

In multicast implementations, the following types of tables implement multicast routing and forwarding:

- **Multicast routing table of a multicast routing protocol**—Each multicast routing protocol has its own multicast routing table, such as PIM routing table.
- **General multicast routing table**—The multicast routing information of different multicast routing protocols forms a general multicast routing table.
- **Multicast forwarding table**—The multicast forwarding table guides the forwarding of multicast packets.

A multicast routing table consists of a set of (S, G) entries. Each entry indicates the routing information for delivering multicast data from a multicast source to a multicast group. If a router supports multiple multicast protocols, its multicast routing table includes routes generated by multiple protocols. The router chooses the optimal route from the multicast routing table based on the configured multicast routing and forwarding policy and adds the route entry to its multicast forwarding table.

The term "router" in this document refers to both routers and Layer 3 switches.

The term "interface" in the multicast routing and forwarding features collectively refers to Layer 3 interfaces, including VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

RPF check mechanism

A multicast routing protocol relies on the existing unicast routes, MBGP routes, or static multicast routes in creating multicast routing entries. When creating multicast routing table entries, a multicast routing protocol uses the reverse path forwarding (RPF) check mechanism to ensure multicast data delivery along the correct paths. In addition, the RPF check mechanism also helps avoid data loops.

RPF check process

The basis for an RPF check is as follows:

- **Unicast routing table**—Contains the shortest path to each destination subnet.
- **MBGP routing table**—Contains multicast routing information.

- **Static multicast routing table**—Contains the RPF routing information defined by the user through static configuration.

MBGP multicast routing table and static multicast routing table are used for RPF check rather than multicast routing.

When a router performs an RPF check, it searches its unicast routing table, MBGP routing table, and static multicast routing table at the same time. The specific process is as follows:

1. The router chooses an optimal route from the unicast routing table, the MBGP routing table, and the static multicast routing table:
 - The router automatically chooses an optimal unicast route by searching its unicast routing table, and using the IP address of the packet source as the destination address. The outgoing interface in the corresponding routing entry is the RPF interface and the next hop is the RPF neighbor. The router considers the path along which the packet from the RPF neighbor arrived on the RPF interface to be the shortest path that leads back to the source.
 - The router automatically chooses an optimal MBGP route by searching its MBGP routing table, and using the IP address of the packet source as the destination address. The outgoing interface in the corresponding routing entry is the RPF interface and the next hop is the RPF neighbor.
 - The router automatically chooses an optimal static multicast route by searching its static multicast routing table, and using the IP address of the packet source as the destination address. The corresponding routing entry explicitly defines the RPF interface and the RPF neighbor.
2. The router selects one of these optimal routes as the RPF route. The selection process is as follows:
 - If configured to use the longest match principle, the router selects the longest match route from these optimal routes. If the three routes have the same mask, the router selects the route with the highest priority. If the three routes have the same priority, the router selects a route as the RPF route according to the sequence of static multicast route, MBGP route, and unicast route.
 - If not configured to use the longest match principle, the router selects the route with the highest priority. If the three routes have the same priority, the router selects a route as the RPF route according to the sequence of static multicast route, MBGP route, and unicast route.

RPF check process

The basis for an RPF check is as follows:

- **Unicast routing table**—Contains the shortest path to each destination subnet.
- **Static multicast routing table**—Contains the RPF routing information defined by the user through static configuration.

When a router performs an RPF check, it searches its unicast routing table, and static multicast routing table at the same time. The specific process is as follows:

1. The router chooses an optimal route from the unicast routing table, and static multicast routing table:
 - The router automatically chooses an optimal unicast route by searching its unicast routing table, and using the IP address of the packet source as the destination address. The outgoing

interface in the corresponding routing entry is the RPF interface and the next hop is the RPF neighbor. The router considers the path along which the packet from the RPF neighbor arrived on the RPF interface to be the shortest path that leads back to the source.

- The router automatically chooses an optimal static multicast route by searching its static multicast routing table, and using the IP address of the packet source as the destination address. The corresponding routing entry explicitly defines the RPF interface and the RPF neighbor.
2. The router selects one of these optimal routes as the RPF route. The selection process is as follows:
 - If configured to use the longest match principle, the router selects the longest match route from the optimal routes. If these routes have the same mask, the router selects the route with the highest priority. If the routes have the same priority, the router selects a route as the RPF route according to the sequence of static multicast route, and unicast route.
 - If not configured to use the longest match principle, the router selects the route with the highest priority. If the routes have the same priority, the router selects a route as the RPF route according to the sequence of static multicast route, and unicast route.

The "packet source" means different things in different situations:

- For a packet traveling along the shortest path tree (SPT) from the multicast source to the receivers or the rendezvous point (RP), the packet source for RPF check is the multicast source.
- For a packet traveling along the rendezvous point tree (RPT) from the RP to the receivers, or along the source-side RPT from the multicast source to the RP, the packet source for RPF check is the RP.
- For a bootstrap message from the bootstrap router (BSR), the packet source for RPF check is the BSR.

For more information about the concepts of SPT, RPT, source-side RPT, RP, and BSR, see "[Configuring PIM \(available only on the HP 5500 EI\)](#)."

RPF check implementation in multicast

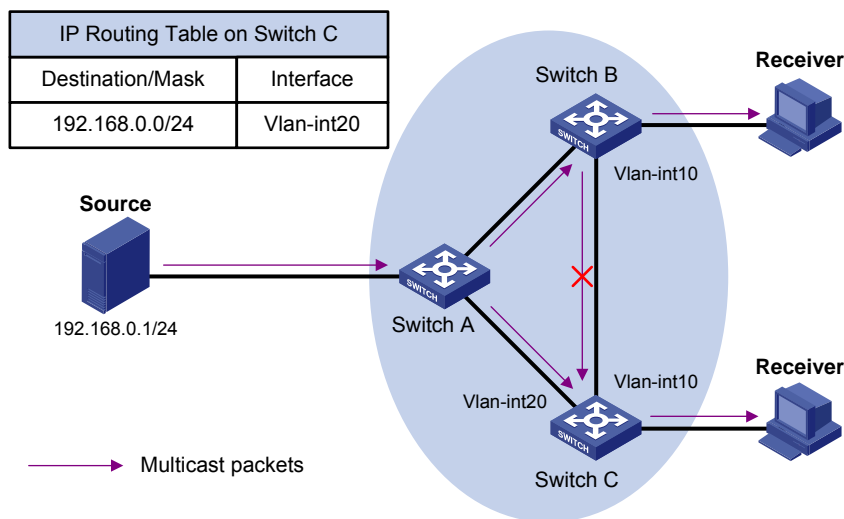
Implementing an RPF check on each received multicast data packet would be a big burden to the router. The use of a multicast forwarding table is the solution to this issue. When creating a multicast routing entry and a multicast forwarding entry for a multicast packet, the router sets the RPF interface of the packet as the incoming interface of the (S, G) entry. After receiving an (S, G) multicast packet, the router first searches its multicast forwarding table:

1. If the corresponding (S, G) entry does not exist in the multicast forwarding table, the packet undergoes an RPF check. The router creates a multicast routing entry based on the relevant routing information and adds the entry into the multicast forwarding table, with the RPF interface as the incoming interface.
 - If the interface that received the packet is the RPF interface, the RPF check succeeds and the router forwards the packet to all the outgoing interfaces.
 - If the interface that received the packet is not the RPF interface, the RPF check fails and the router discards the packet.
2. If the corresponding (S, G) entry exists, and the interface that received the packet is the incoming interface, the router forwards the packet to all the outgoing interfaces.

3. If the corresponding (S, G) entry exists, but the interface that received the packet is not the incoming interface in the multicast forwarding table, the multicast packet undergoes an RPF check.
 - If the RPF interface is the incoming interface of the (S, G) entry, it indicates that the (S, G) entry is correct but the packet arrived from a wrong path. The packet will be discarded.
 - If the RPF interface is not the incoming interface, it indicates that the (S, G) entry has expired, and router replaces the incoming interface with the RPF interface. If the interface on which the packet arrived is the RPF interface, the router forwards the packet to all the outgoing interfaces. Otherwise, it discards the packet.

Assume that unicast routes are available in the network, MBGP is not configured, and no static multicast routes have been configured on Switch C, as shown in Figure 26. Multicast packets travel along the SPT from the multicast source to the receivers. The multicast forwarding table on Switch C contains the (S, G) entry, with VLAN-interface 20 as the incoming interface.

Figure 26 RPF check process



- When a multicast packet arrives on interface VLAN-interface 20 of Switch C, because the interface is the incoming interface of the (S, G) entry, the router forwards the packet to all outgoing interfaces.
- When a multicast packet arrives on interface VLAN-interface 10 of Switch C, because the interface is not the incoming interface of the (S, G) entry, the router performs an RPF check on the packet. The router searches its unicast routing table and finds that the outgoing interface to Source (the RPF interface) is VLAN-interface 20. This means the (S, G) entry is correct, and packet arrived along a wrong path. The RPF check fails and the packet is discarded.

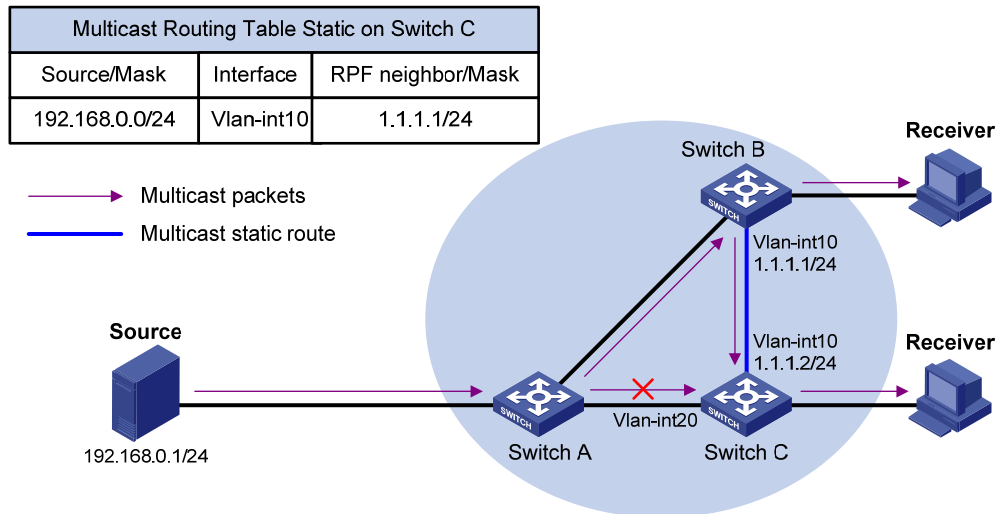
Static multicast routes

A static multicast route is an important basis for RPF check. Depending on the application environment, a static multicast route can change an RPF route and create an RPF route.

Changing an RPF route

Typically, the topology structure of a multicast network is the same as that of a unicast network, and multicast traffic follows the same transmission path as unicast traffic does. You can configure a static multicast route for a given multicast source to change the RPF route to create a transmission path for multicast traffic that is different from that for unicast traffic.

Figure 27 Changing an RPF route

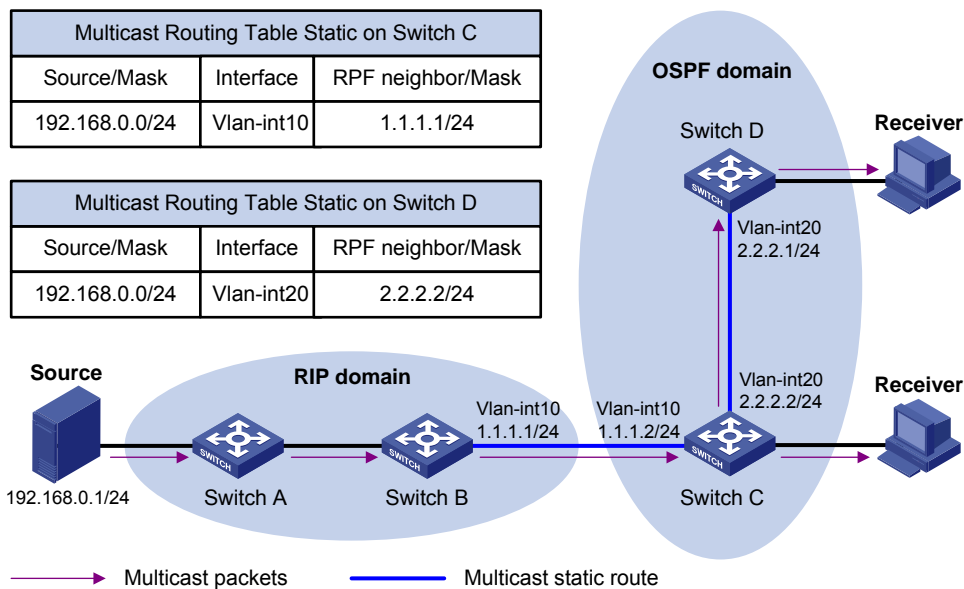


As shown in Figure 27, when no static multicast route is configured, Switch C's RPF neighbor on the path back to Source is Switch A. The multicast information from Source travels along the path from Switch A to Switch C, which is the unicast route between the two routers. When a static multicast route is configured on Switch C and Switch B is configured as Switch C's RPF neighbor on the path back to Source, the multicast information from Source travels from Switch A to Switch B and then to Switch C.

Creating an RPF route

When a unicast route is blocked, multicast traffic forwarding might be stopped because of lack of an RPF route. By configuring a static multicast route for a given multicast source, you can create an RPF route so that a multicast routing entry is created to guide multicast traffic forwarding regardless of whether a unicast route is available.

Figure 28 Creating an RPF route



As shown in [Figure 28](#), the RIP domain and the OSPF domain are unicast isolated from each other. When no static multicast route is configured, the hosts (the receivers) in the OSPF domain cannot receive the multicast packets that the multicast source (the source) sent in the RIP domain. After you configure a static multicast route on Switch C and Switch D, specifying Switch B as the RPF neighbor of Switch C and specifying Switch C as the RPF neighbor of Switch D, the receivers can receive multicast data that the multicast source sent.

NOTE:

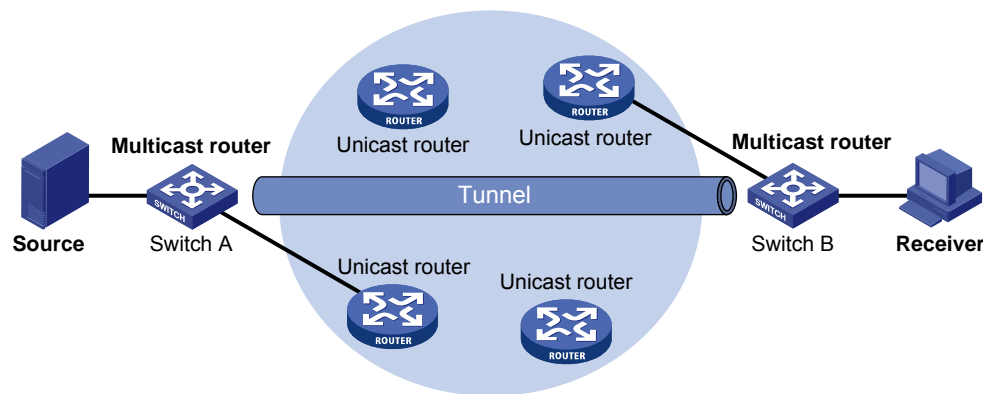
- Static multicast routes only affect RPF check but cannot guide multicast forwarding.
- A static multicast route is effective only on the multicast router on which it is configured, and will not be advertised throughout the network or redistributed to other routers.

Multicast forwarding across unicast subnets

Some networking devices might not support multicast protocols in a network. Multicast devices forward multicast traffic from a multicast source hop by hop along the forwarding tree. When the multicast traffic is forwarded to a next-hop device that does not support IP multicast, the forwarding path is blocked. In this case, you can enable multicast traffic forwarding across the unicast subnet by establishing a tunnel, such as an IPv4 over IPv4 tunnel, between the devices at both ends of the unicast subnet.

For more information about tunneling, see *Layer 3—IP Services Configuration Guide*.

Figure 29 Multicast data transmission through a tunnel



As shown in Figure 29, with tunnel established between Switch A and Switch B, Switch A encapsulates multicast data in unicast IP packets, which unicast routers then forward to Switch B across the tunnel. Then, Switch B strips off the unicast IP header and continues to forward the multicast data down toward the receivers.

If unicast static routes are configured across the tunnel, any unicast packet can be transmitted through the tunnel. If you want to dedicate this tunnel to multicast traffic delivery, you can configure only a static multicast route across the tunnel, so that only multicast packets are transmitted through this tunnel.

Multicast traceroute

You can use the multicast traceroute utility to trace the path that a multicast stream flows down from the first-hop router to the last-hop router.

Concepts in multicast traceroute

- **Last-hop router**—If one of the interfaces of a router connects to the subnet that contains the given destination address, and if the router can forward multicast streams from the given multicast source onto that subnet, that router is called the "last-hop router".
- **First-hop router**—The router that directly connects to the multicast source is called the "first-hop router".
- **Querier**—The router that sends multicast traceroute requests is called the "querier".

Introduction to multicast traceroute packets

A multicast traceroute packet is a special IGMP packet that is different from common IGMP packets in that its IGMP Type field is set to 0x1F or 0x1E and its destination IP address is a unicast address. The following types of multicast traceroute packets are available:

- Query, with the IGMP Type field set to 0x1F,
- Request, with the IGMP Type field set to 0x1F, and
- Response, with the IGMP Type field set to 0x1E.

Process of multicast traceroute

1. The querier sends a query to the last-hop router.
2. After receiving the query, the last-hop router turns the query packet into a request packet by adding a response data block (which contains its interface addresses and packet statistics) to the end of the packet. It then forwards the request packet through unicast to the previous hop for the given multicast source and group.
3. From the last-hop router to the multicast source, each hop adds a response data block to the end of the request packet and unicasts it to the previous hop.
4. When the first-hop router receives the request packet, it changes the packet type to indicate a response packet. Then, it sends the completed packet through unicast to the querier.

Configuration task list

Task	Remarks	
Enabling IP multicast routing	Required	
	Configuring static multicast routes	Optional
	Configuring a multicast routing policy	Optional
Configuring multicast routing and forwarding	Configuring a multicast forwarding range	Optional
	Configuring the multicast forwarding table size	Optional
	Tracing a multicast path	Optional

ⓘ IMPORTANT:

IP multicast does not support secondary IP address segments. Namely, multicast can be routed and forwarded only through primary IP addresses even if secondary addresses are configured on the ports. For more information about primary and secondary IP addresses, see *Layer 3— IP Services Configuration Guide*.

Enabling IP multicast routing

Before you configure any Layer 3 multicast functionality, you must enable IP multicast routing.

Enabling IP multicast routing for the public network

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IP multicast routing.	multicast routing-enable	Disabled by default

Enabling IP multicast routing in a VPN instance

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a VPN instance and enter VPN instance view.	ip vpn-instance <i>vpn-instance-name</i>	N/A
3. Configure a route distinguisher (RD) for the VPN instance.	route-distinguisher <i>route-distinguisher</i>	No RD is configured by default.
4. Enable IP multicast routing.	multicast routing-enable	Disabled by default.

For more information about the **ip vpn-instance** and **route-distinguisher** commands, see *IP Routing Command Reference*.

Configuring multicast routing and forwarding

Before you configure multicast routing and forwarding, complete the following tasks:

- Configure a unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Enable PIM (PIM-DM or PIM-SM).
- Determine the maximum number of downstream nodes for a single multicast forwarding table entry.
- Determine the maximum number of entries in the multicast forwarding table.

Configuring static multicast routes

By configuring a static multicast route for a given multicast source, you can specify an RPF interface or an RPF neighbor for multicast traffic from that source. If you want to remove a specific static multicast route, use the **undo ip rpf-route-static** command, if you want to remove all static multicast routes, use the **delete ip rpf-route-static** command.

When you configure a static multicast route, you cannot specify an RPF neighbor by providing the type and number (*interface-type interface-number*) of the interface if the interface of the RPF neighbor is a Layer 3 Ethernet interface, Layer 3 aggregate interface, Loopback interface, or VLAN interface. Instead, you can specify such an RPF neighbor only by its address (*rpf-nbr-address*).

To configure a static multicast route:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure a static multicast route.	ip rpf-route-static [vpn-instance <i>vpn-instance-name</i>] <i>source-address</i> { <i>mask</i> <i>mask-length</i> } [<i>protocol</i> [<i>process-id</i>]] [route-policy <i>policy-name</i>] { <i>rpf-nbr-address</i> <i>interface-type interface-number</i> } [preference <i>preference</i>] [order <i>order-number</i>]	No static multicast route is configured by default.

Step	Command	Remarks
3. Delete static multicast routes.	delete ip rpf-route-static [vpn-instance vpn-instance-name]	Optional.

Configuring a multicast routing policy

You can configure the router to determine the RPF route based on the longest match principle. For more information about RPF route selection, see "[RPF check process](#)."

By configuring per-source or per-source-and-group load splitting, you can optimize the traffic delivery when multiple data flows are handled.

Configuring a multicast routing policy for the public network

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the device to select the RPF route based on the longest match.	multicast longest-match	The route with the highest priority is selected as the RPF route by default.
3. Configure multicast load splitting.	multicast load-splitting { source source-group }	Optional. Disabled by default. This command does not take effect in BIDIR-PIM.

Configuring a multicast routing policy in a VPN instance

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VPN instance view.	ip vpn-instance vpn-instance-name	N/A
3. Configure the device to select the RPF route based on the longest match.	multicast longest-match	The route with the highest priority is selected as the RPF route by default.
4. Configure multicast load splitting.	multicast load-splitting { source source-group }	Optional. Disabled by default. This command does not take effect in BIDIR-PIM.

Configuring a multicast forwarding range

Multicast packets do not travel without a boundary in a network. The multicast data corresponding to each multicast group must be transmitted within a definite scope.

You can configure a forwarding boundary specific to a particular multicast group on all interfaces that support multicast forwarding. A multicast forwarding boundary sets the boundary condition for the

multicast groups in the specified range. If the destination address of a multicast packet matches the set boundary condition, the packet will not be forwarded. After you configure an interface as a multicast boundary, the interface can no longer forward multicast packets—including packets sent from the local device—or receive multicast packets.

To configure a multicast forwarding range:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure a multicast forwarding boundary.	multicast boundary <i>group-address</i> { <i>mask</i> <i>mask-length</i> }	No forwarding boundary by default.

Configuring the multicast forwarding table size

The switch maintains the corresponding forwarding entry for each multicast packet that it receives. Excessive multicast routing entries, however, can exhaust the switch's memory and cause lower performance. You can set a limit on the number of entries in the multicast forwarding table based on the networking situation and the performance requirements. If the configured maximum number of multicast forwarding table entries is smaller than the current value, the forwarding entries in excess are not deleted immediately. Instead, the multicast routing protocol that runs on the switch deletes them. The switch no longer adds new multicast forwarding entries until the number of existing multicast forwarding entries comes down below the configured value.

When forwarding multicast traffic, the switch replicates a copy of the multicast traffic for each downstream node and forwards the traffic. Therefore, each of these downstream nodes forms a branch of the multicast distribution tree. You can configure the maximum number of downstream nodes (the maximum number of outgoing interfaces), for a single entry in the multicast forwarding table to lessen the burden on the switch for replicating multicast traffic. If the configured maximum number of downstream nodes for a single multicast forwarding entry is smaller than the current number, the downstream nodes in excess are not deleted immediately. Instead, the multicast routing protocol that runs on the switch deletes them. The switch no longer adds new multicast forwarding entries for newly added downstream nodes until the number of existing downstream nodes comes down below the configured value.

Configuring the multicast forwarding table size for the public network

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the maximum number of entries in the multicast forwarding table.	multicast forwarding-table route-limit <i>limit</i>	Optional. 2000 by default.

Step	Command	Remarks
3. Configure the maximum number of downstream nodes for a single multicast forwarding entry.	multicast forwarding-table downstream-limit <i>limit</i>	Optional. 128 by default.

Configuring the multicast forwarding table size in a VPN instance

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VPN instance view.	ip vpn-instance <i>vpn-instance-name</i>	N/A
3. Configure the maximum number of entries in the multicast forwarding table.	multicast forwarding-table route-limit <i>limit</i>	Optional. 2000 by default.
4. Configure the maximum number of downstream nodes for a single route in the multicast forwarding table.	multicast forwarding-table downstream-limit <i>limit</i>	Optional. 128 by default.

Tracing a multicast path

You can run the **mtracert** command to trace the path down which the multicast traffic flows from a given first-hop router to the last-hop router.

To trace a multicast path:

Task	Command	Remarks
Trace a multicast path.	mtracert <i>source-address</i> [[<i>last-hop-router-address</i>] <i>group-address</i>]	Available in any view

Displaying and maintaining multicast routing and forwarding

△ CAUTION:

The **reset** commands might cause multicast data transmission failures.

To display and maintain multicast routing and forwarding:

Task	Command	Remarks
Display multicast boundary information.	display multicast [all-instance vpn-instance <i>vpn-instance-name</i>] boundary [<i>group-address</i> [<i>mask</i> <i>mask-length</i>]] [interface <i>interface-type</i> <i>interface-number</i>] [[{ begin exclude include } <i>regular-expression</i>]]	Available in any view.
Display multicast forwarding table information.	display multicast [all-instance vpn-instance <i>vpn-instance-name</i>] forwarding-table [<i>source-address</i> [mask { <i>mask</i> <i>mask-length</i> }] <i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }]] incoming-interface { <i>interface-type</i> <i>interface-number</i> register } outgoing-interface { exclude include match } { <i>interface-type</i> <i>interface-number</i> register } statistics slot <i>slot-number</i>] * [port-info] [[{ begin exclude include } <i>regular-expression</i>]]	Available in any view.
Display the DF information of the multicast forwarding table.	display multicast [all-instance vpn-instance <i>vpn-instance-name</i>] forwarding-table df-info [<i>rp-address</i>] [slot <i>slot-number</i>] [[{ begin exclude include } <i>regular-expression</i>]]	Available in any view.
Display information about the multicast routing table.	display multicast [all-instance vpn-instance <i>vpn-instance-name</i>] routing-table [<i>source-address</i> [mask { <i>mask</i> <i>mask-length</i> }] <i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }]] incoming-interface { <i>interface-type</i> <i>interface-number</i> register } outgoing-interface { exclude include match } { <i>interface-type</i> <i>interface-number</i> register }] * [[{ begin exclude include } <i>regular-expression</i>]]	Available in any view.
Display information about the static multicast routing table.	display multicast routing-table [all-instance vpn-instance <i>vpn-instance-name</i>] static [<i>source-address</i> { <i>mask-length</i> <i>mask</i> }] [[{ begin exclude include } <i>regular-expression</i>]]	Available in any view.
Display RPF route information about the specified multicast source.	display multicast [all-instance vpn-instance <i>vpn-instance-name</i>] rpf-info <i>source-address</i> [<i>group-address</i>] [[{ begin exclude include } <i>regular-expression</i>]]	Available in any view.
Clear forwarding entries from the multicast forwarding table.	reset multicast [all-instance vpn-instance <i>vpn-instance-name</i>] forwarding-table { { <i>source-address</i> [mask { <i>mask</i> <i>mask-length</i> }] <i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }]] incoming-interface { <i>interface-type</i> <i>interface-number</i> register } } * [all]	Available in user view. When a forwarding entry is deleted from the multicast forwarding table, the corresponding routing entry is also deleted from the multicast routing table.

Task	Command	Remarks
Clear routing entries from the multicast routing table.	reset multicast [all-instance vpn-instance <i>vpn-instance-name</i>] routing-table { { <i>source-address</i> [mask { <i>mask</i> <i>mask-length</i> }] <i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }] incoming-interface { <i>interface-type interface-number</i> register } } * all }	Available in user view. When a routing entry is deleted from the multicast routing table, the corresponding forwarding entry is also deleted from the multicast forwarding table.

For more information about designated forwarder (DF), see "[Configuring PIM \(available only on the HP 5500 EI\)](#)."

Configuration examples

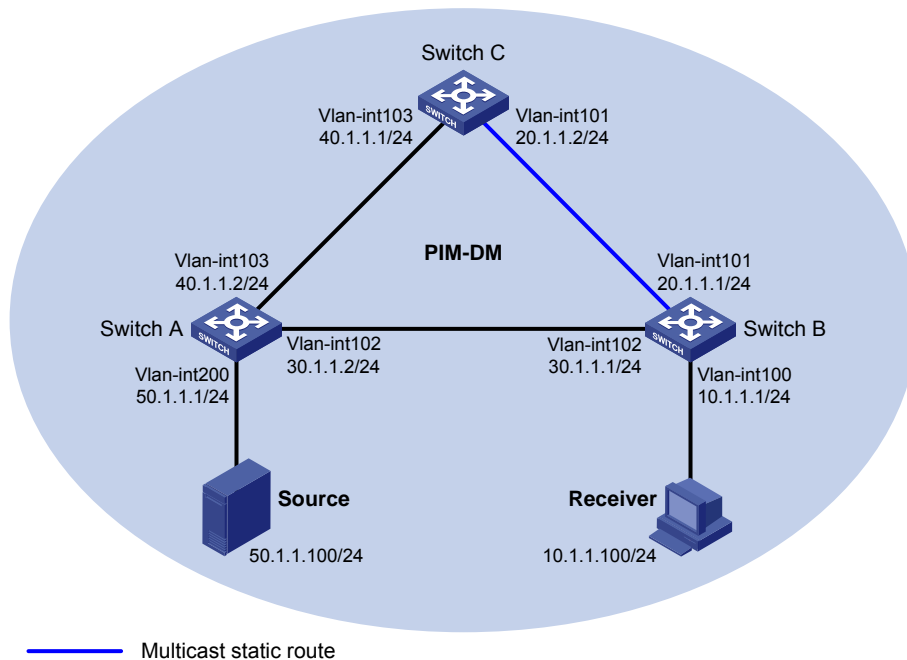
Changing an RPF route

Network requirements

PIM-DM runs in the network. All switches in the network support multicast. Switch A, Switch B, and Switch C run OSPF. Typically, Receiver can receive the multicast data from Source through the path: Switch A to Switch B, which is the same as the unicast route.

Perform the following configuration so that Receiver can receive the multicast data from Source through the path: Switch A to Switch C to Switch B, which is different from the unicast route.

Figure 30 Network diagram



Configuration procedure

1. Configure the IP address and subnet mask for each interface as per Figure 30. (Details not shown.)
2. Enable OSPF on the switches in the PIM-DM domain to make sure the switches are interoperable at the network layer and they can dynamically update their routing information. (Details not shown.)
3. Enable IP multicast routing, IGMP and PIM-DM:

Enable IP multicast routing on Switch B, enable IGMP on VLAN-interface 100, and enable PIM-DM on each interface.

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp enable
[SwitchB-Vlan-interface100] pim dm
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim dm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim dm
[SwitchB-Vlan-interface102] quit
```

Enable IP multicast routing on Switch A, and enable PIM-DM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] pim dm
```

```
[SwitchA-Vlan-interface200] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim dm
[SwitchA-Vlan-interface102] quit
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim dm
[SwitchA-Vlan-interface103] quit

# Enable IP multicast routing and PIM-DM on Switch C in the same way. (Details not shown.)

# Use the display multicast rpf-info command to display the RPF route to Source on Switch B.
[SwitchB] display multicast rpf-info 50.1.1.100
RPF information about source 50.1.1.100:
  RPF interface: Vlan-interface102, RPF neighbor: 30.1.1.2
  Referenced route/mask: 50.1.1.0/24
  Referenced route type: igp
  Route selection rule: preference-preferred
  Load splitting rule: disable
```

The output shows that the current RPF route on Switch B is contributed by a unicast routing protocol and the RPF neighbor is Switch A.

4. Configure a static multicast route on Switch B, specifying Switch C as its RPF neighbor on the route to Source.

```
[SwitchB] ip rpf-route-static 50.1.1.100 24 20.1.1.2
```

Verifying the configuration

- # Display information about the RPF route to Source on Switch B.

```
[SwitchB] display multicast rpf-info 50.1.1.100
RPF information about source 50.1.1.100:
  RPF interface: Vlan-interface101, RPF neighbor: 20.1.1.2
  Referenced route/mask: 50.1.1.0/24
  Referenced route type: static multicast
  Route selection rule: preference-preferred
  Load splitting rule: disable
```

The output shows that the RPF route on Switch B has changed. It is now the configured static multicast route, and the RPF neighbor is now Switch C.

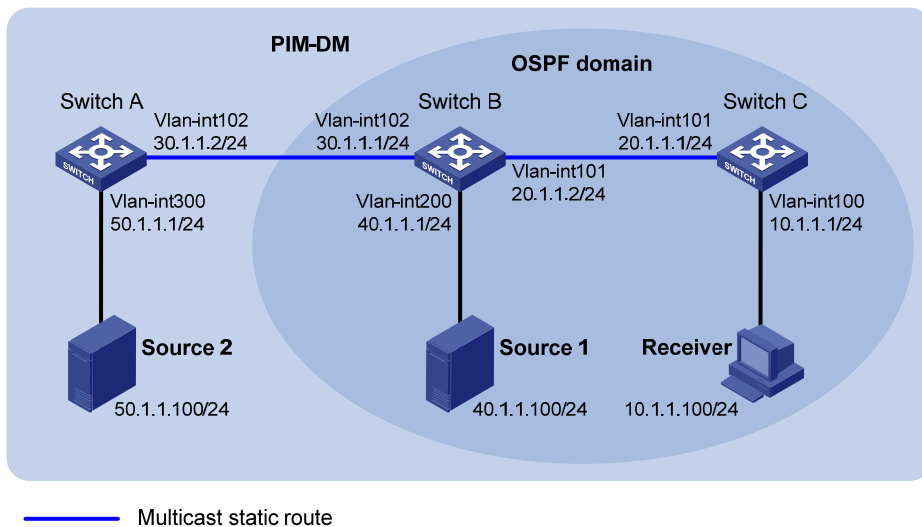
Creating an RPF route

Network requirements

PIM-DM runs in the network and all switches in the network support IP multicast. Switch B and Switch C run OSPF, and have no unicast routes to Switch A. Typically, Receiver can receive the multicast data from Source 1 in the OSPF domain.

Perform the following configuration so that Receiver can receive multicast data from Source 2, which is outside the OSPF domain.

Figure 31 Network diagram



Configuration procedure

1. Configure the IP address and subnet mask for each interface as per Figure 31. (Details not shown.)
2. Enable OSPF on Switch B and Switch C to make sure they are interoperable at the network layer and they can dynamically update their routing information. (Details not shown.)
3. Enable IP multicast routing, and enable PIM-DM and IGMP:

Enable IP multicast routing on Switch C, enable PIM-DM on each interface, and enable IGMP on VLAN-interface 100.

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] igmp enable
[SwitchC-Vlan-interface100] pim dm
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 101
[SwitchC-Vlan-interface101] pim dm
[SwitchC-Vlan-interface101] quit
```

Enable IP multicast routing on Switch A and enable PIM-DM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 300
[SwitchA-Vlan-interface300] pim dm
[SwitchA-Vlan-interface300] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim dm
[SwitchA-Vlan-interface102] quit
```

Enable IP multicast routing and PIM-DM on Switch B in the same way. (Details not shown.)

Use the **display multicast rpf-info** command to display the RPF routes to Source 2 on Switch B and Switch C.

```
[SwitchB] display multicast rpf-info 50.1.1.100
```

```
[SwitchC] display multicast rpf-info 50.1.1.100
```

No information is displayed. This means that no RPF route to Source 2 exists on Switch B or Switch C.

4. Configure a static multicast route:

Configure a static multicast route on Switch B, specifying Switch A as its RPF neighbor on the route to Source 2.

```
[SwitchB] ip rpf-route-static 50.1.1.100 24 30.1.1.2
```

Configure a static multicast route on Switch C, specifying Switch B as its RPF neighbor on the route to Source 2.

```
[SwitchC] ip rpf-route-static 10.1.1.100 24 20.1.1.2
```

Verifying the configuration

Display the RPF routes to Source 2 on Switch B and Switch C.

```
[SwitchB] display multicast rpf-info 50.1.1.100
```

```
RPF information about source 50.1.1.100:
```

```
  RPF interface: Vlan-interface102, RPF neighbor: 30.1.1.2
```

```
  Referenced route/mask: 50.1.1.0/24
```

```
  Referenced route type: static multicast
```

```
  Route selection rule: preference-preferred
```

```
  Load splitting rule: disable
```

```
[SwitchC] display multicast rpf-info 50.1.1.100
```

```
RPF information about source 50.1.1.100:
```

```
  RPF interface: Vlan-interface101, RPF neighbor: 20.1.1.2
```

```
  Referenced route/mask: 50.1.1.0/24
```

```
  Referenced route type: static multicast
```

```
  Route selection rule: preference-preferred
```

```
  Load splitting rule: disable
```

The output shows that the RPF routes to Source 2 exist on Switch B and Switch C. The routes are the configured static routes.

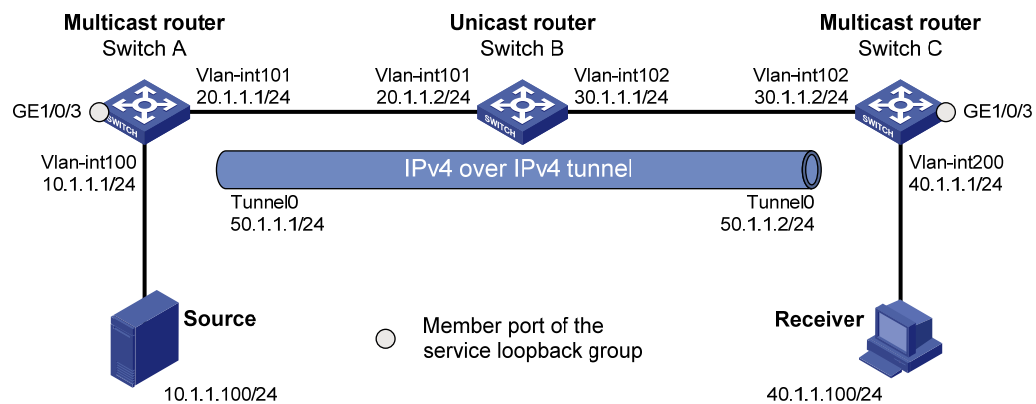
Multicast forwarding over a tunnel

Network requirements

Multicast routing and PIM-DM are enabled on Switch A and Switch C. Switch B does not support multicast. OSPF runs on Switch A, Switch B, and Switch C.

Perform the following configurations so that Receiver can receive the multicast data from Source.

Figure 32 Network diagram



Configuration procedure

1. Configure the IP address and subnet mask for each interface as per Figure 32. (Details not shown.)
2. Configure an IPv4 over IPv4 tunnel:

Create service loopback group 1 on Switch A and specify its service type as Tunnel.

```
<SwitchA> system-view
[SwitchA] service-loopback group 1 type tunnel
```

Disable STP, LLDP and NDP on interface GigabitEthernet 1/0/3 of Switch A, and add the interface to service loopback group 1. GigabitEthernet 1/0/3 does not belong to VLAN 100 or VLAN 101.

```
[SwitchA] interface gigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] undo stp enable
[SwitchA-GigabitEthernet1/0/3] undo ndp enable
[SwitchA-GigabitEthernet1/0/3] undo lldp enable
[SwitchA-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchA-GigabitEthernet1/0/3] quit
```

Create interface Tunnel 0 on Switch A, assign the IP address and subnet mask to the interface Tunnel 0, and reference service loopback group 1 on interface Tunnel 0.

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ip address 50.1.1.1 24
[SwitchA-Tunnel0] service-loopback-group 1
```

Specify the tunnel encapsulation mode as IPv4 over IPv4 and assign the source and destination addresses to the interface.

```
[SwitchA-Tunnel0] tunnel-protocol ipv4-ipv4
[SwitchA-Tunnel0] source 20.1.1.1
[SwitchA-Tunnel0] destination 30.1.1.2
[SwitchA-Tunnel0] quit
```

Create service loopback group 1 on Switch C and specify its service type as Tunnel.

```
<SwitchC> system-view
[SwitchC] service-loopback group 1 type tunnel
```

Disable STP, LLDP and NDP on interface GigabitEthernet 1/0/3 of Switch C, and add the interface to service loopback group 1. GigabitEthernet 1/0/3 does not belong to VLAN 200 or VLAN 102.

```
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] undo stp enable
[SwitchC-GigabitEthernet1/0/3] undo ndp enable
[SwitchC-GigabitEthernet1/0/3] undo lldp enable
[SwitchC-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchC-GigabitEthernet1/0/3] quit
```

Create interface Tunnel 0 on Switch C, assign the IP address and subnet mask to the interface Tunnel 0, and reference service loopback group 1 on interface Tunnel 0.

```
[SwitchC] interface tunnel 0
[SwitchC-Tunnel0] ip address 50.1.1.2 24
[SwitchC-Tunnel0] service-loopback-group 1
```

Specify the tunnel encapsulation mode as IPv4 over IPv4 and assign the source and destination addresses to the interface.

```
[SwitchC-Tunnel0] tunnel-protocol ipv4-ipv4
[SwitchC-Tunnel0] source 20.1.1.1
[SwitchC-Tunnel0] destination 30.1.1.2
[SwitchC-Tunnel0] quit
```

3. Configure OSPF:

Configure OSPF on Switch A.

```
[SwitchA] ospf 1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 50.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

Configure OSPF on Switch B.

```
<SwitchB> system-view
[SwitchB] ospf 1
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Configure OSPF on Switch C.

```
[SwitchC] ospf 1
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 50.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

4. Enable IP multicast routing, PIM-DM, and IGMP:

Enable multicast routing on Switch A and enable PIM-DM on each interface.

```
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim dm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] pim dm
[SwitchA-Tunnel0] quit
```

Enable multicast routing on Switch C, enable PIM-DM on each interface, and enable IGMP on VLAN-interface 200.

```
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] igmp enable
[SwitchC-Vlan-interface200] pim dm
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 102
[SwitchC-Vlan-interface102] pim dm
[SwitchC-Vlan-interface102] quit
[SwitchC] interface tunnel 0
[SwitchC-Tunnel0] pim dm
[SwitchC-Tunnel0] quit
```

5. On Switch C, configure a static multicast route, specifying the RPF neighbor leading toward Source as Tunnel 0 on Switch A.

```
[SwitchC] ip rpf-route-static 50.1.1.0 24 50.1.1.1
```

Verifying the configuration

Source sends multicast data to the multicast group 225.1.1.1 and Receiver can receive the multicast data after joining the multicast group. You can view the PIM routing table information on routers using the **display pim routing-table** command. For example:

Display the PIM routing table information on Switch C.

```
[SwitchC] display pim routing-table
VPN-Instance: public net
Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
  Protocol: pim-dm, Flag: WC
  UpTime: 00:04:25
  Upstream interface: NULL
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
```



```

1: Vlan-interface200
    Protocol: igmp, UpTime: 00:04:25, Expires: never

(10.1.1.100, 225.1.1.1)
    Protocol: pim-dm, Flag: ACT
    UpTime: 00:06:14
    Upstream interface: Tunnel0
        Upstream neighbor: 50.1.1.1
        RPF prime neighbor: 50.1.1.1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlan-interface200
            Protocol: pim-dm, UpTime: 00:04:25, Expires: never

```

The output shows that Switch A is the RPF neighbor of Switch C and the multicast data from Switch A is delivered over an IPv4 over IPv4 tunnel to Switch C.

Troubleshooting multicast routing and forwarding

Static multicast route failure

Symptom

No dynamic routing protocol is enabled on the routers, and the physical status and link layer status of interfaces are both up, but the static multicast route fails.

Analysis

- If the static multicast route is not configured or updated correctly to match the current network conditions, the route entry and the configuration information of static multicast route do not exist in the multicast routing table.
- If a better route is found, the static multicast route might also fail.

Solution

1. Use the **display multicast routing-table static** command to view the information of static multicast routes to verify that the static multicast route has been correctly configured and that the route entry exists in the multicast routing table.
2. Check the type of the next hop interface of the static multicast route. If the interface is not a point-to-point interface, be sure to specify the next hop address for the outgoing interface when you configure the static multicast route.
3. Check that the static multicast route matches the specified routing protocol. If a protocol was specified in static multicast route configuration, enter the **display ip routing-table** command to check if an identical route was added by the protocol.
4. Check that the static multicast route matches the specified routing policy. If a routing policy was specified when the static multicast route was configured, enter the **display route-policy** command to check the configured routing policy.

Multicast data fails to reach receivers

Symptom

The multicast data can reach some routers but fails to reach the last-hop router.

Analysis

If a multicast forwarding boundary has been configured through the **multicast boundary** command, any multicast packet will be kept from crossing the boundary.

Solution

1. Use the **display pim routing-table** command to verify that the corresponding (S, G) entries exist on the router. If yes, the router has received the multicast data. Otherwise, the router has not received the data.
2. Use the **display multicast boundary** command to check the multicast boundary information on the interfaces. Use the **multicast boundary** command to change the multicast forwarding boundary setting.
3. In the case of PIM-SM, use the **display current-configuration** command to check the BSR and RP information.

Configuring IGMP (available only on the HP 5500 EI)

Overview

As a TCP/IP protocol responsible for IP multicast group member management, the Internet Group Management Protocol (IGMP) is used by IP hosts and adjacent multicast routers to establish and maintain their multicast group memberships.

The term "router" in this document refers to both routers and Layer 3 switches.

The term "interface" in this chapter collectively refers to Layer 3 interfaces, including VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

IGMP versions

- IGMPv1 (defined in RFC 1112)
- IGMPv2 (defined in RFC 2236)
- IGMPv3 (defined in RFC 3376)

All IGMP versions support the Any-Source Multicast (ASM) model. In addition to the ASM model, IGMPv3 can directly implement the Source-Specific Multicast (SSM) model. IGMPv1 and IGMPv2 must work with the IGMP SSM mapping function to implement the SSM model.

For more information about the ASM and SSM models, see "[Multicast overview](#)."

Introduction to IGMPv1

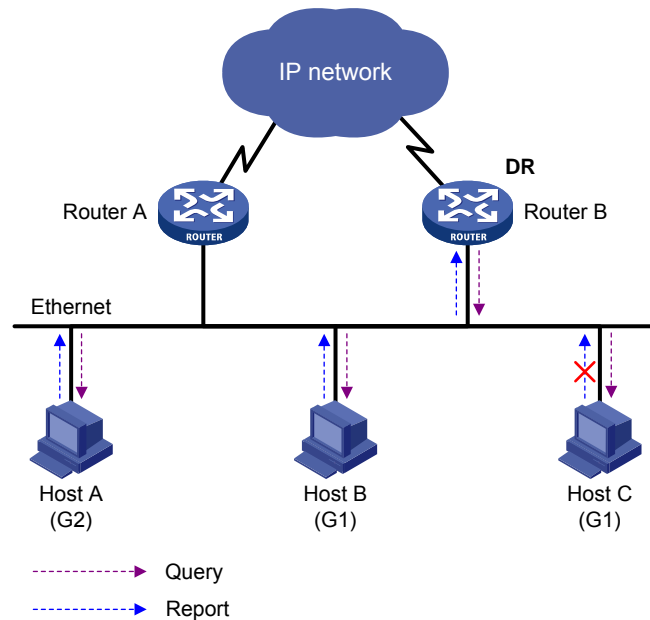
IGMPv1 manages multicast group memberships mainly based on the query and response mechanism.

All multicast routers on the same subnet can receive IGMP membership report messages (often called "reports") from hosts, but the subnet needs only one router to send IGMP query messages (often called "queries"). The querier election mechanism determines which router acts as the IGMP querier on the subnet.

In IGMPv1, the designated router (DR) elected by the working multicast routing protocol (such as PIM) serves as the IGMP querier.

For more information about DR, see "[Configuring PIM \(available only on the HP 5500 EI\)](#)."

Figure 33 IGMP queries and reports



Assume that Host B and Host C are interested in multicast data addressed to multicast group G1, and Host A is interested in multicast data addressed to G2, as shown in Figure 33. The following process describes how the hosts join the multicast groups and how the IGMP querier (Router B in the figure) maintains the multicast group memberships:

1. The hosts send unsolicited IGMP reports to the addresses of the multicast groups that they want to join, without having to wait for the IGMP queries from the IGMP querier.
2. The IGMP querier periodically multicasts IGMP queries (with the destination address of 224.0.0.1) to all hosts and routers on the local subnet.
3. After receiving a query message, Host B or Host C (the delay timer of whichever expires first) sends an IGMP report to the multicast group address of G1, to announce its membership for G1. Assume that Host B sends the report message. After receiving the report from Host B, Host C (which is on the same subnet as Host B) suppresses its own report for G1, because the IGMP routers (Router A and Router B) have already known that at least one host on the local subnet is interested in G1. This IGMP report suppression mechanism helps reduce traffic on the local subnet.
4. At the same time, because Host A is interested in G2, it sends a report to the multicast group address of G2.
5. Through the query/report process, the IGMP routers determine that members of G1 and G2 are attached to the local subnet, and the multicast routing protocol that is running on the routers (PIM, for example) generates (*, G1) and (*, G2) multicast forwarding entries. These entries will be the basis for subsequent multicast forwarding, where asterisk represents any multicast source.

6. When the multicast data addressed to G1 or G2 reaches an IGMP router, because the (*, G1) and (*, G2) multicast forwarding entries exist on the IGMP router, the router forwards the multicast data to the local subnet, and then the receivers on the subnet receive the data.

IGMPv1 does not specifically define a leave group message (often called a "leave message"). When an IGMPv1 host is leaving a multicast group, it stops sending reports to the address of the multicast group that it listened to. If no member exists in a multicast group on the subnet, the IGMP router will not receive any report addressed to that multicast group. In this case, the router will delete the multicast forwarding entries for that multicast group after a period of time.

Enhancements in IGMPv2

Compared with IGMPv1, IGMPv2 has introduced a querier election mechanism and a leave-group mechanism.

Querier election mechanism

In IGMPv1, the DR elected by the Layer 3 multicast routing protocol (such as PIM) serves as the querier among multiple routers on the same subnet.

IGMPv2 introduced an independent querier election mechanism. The querier election process is as follows:

1. Initially, every IGMPv2 router assumes itself as the querier and sends IGMP general query messages (often called "general queries") to all hosts and routers on the local subnet. The destination address is 224.0.0.1.
2. After receiving a general query, every IGMPv2 router compares the source IP address of the query message with its own interface address. After comparison, the router with the lowest IP address wins the querier election, and all other IGMPv2 routers become non-queriers.
3. All the non-queriers start a timer, known as "other querier present timer." If a router receives an IGMP query from the querier before the timer expires, it resets this timer. Otherwise, it assumes the querier to have timed out and initiates a new querier election process.

"Leave group" mechanism

In IGMPv1, when a host leaves a multicast group, it does not send any notification to the multicast router. The multicast router relies on the host response timeout timer to determine whether a group has members. This adds to the leave latency.

In IGMPv2, when a host leaves a multicast group, the following steps occur:

1. This host sends a leave message to all routers on the local subnet. The destination address is 224.0.0.2.
2. After receiving the leave message, the querier sends a configurable number of group-specific queries to the group that the host is leaving. The destination address field and group address field of the message are both filled with the address of the multicast group that is being queried.
3. One of the remaining members (if any on the subnet) of the group that is being queried should send a membership report within the maximum response time set in the query messages.

4. If the querier receives a membership report for the group within the maximum response time, it will maintain the memberships of the group. Otherwise, the querier will assume that no hosts on the subnet are still interested in multicast traffic to that group and will stop maintaining the memberships of the group.

Enhancements in IGMPv3

IGMPv3 is based on and is compatible with IGMPv1 and IGMPv2. It provides hosts with enhanced control capabilities and provides enhancements of query and report messages.

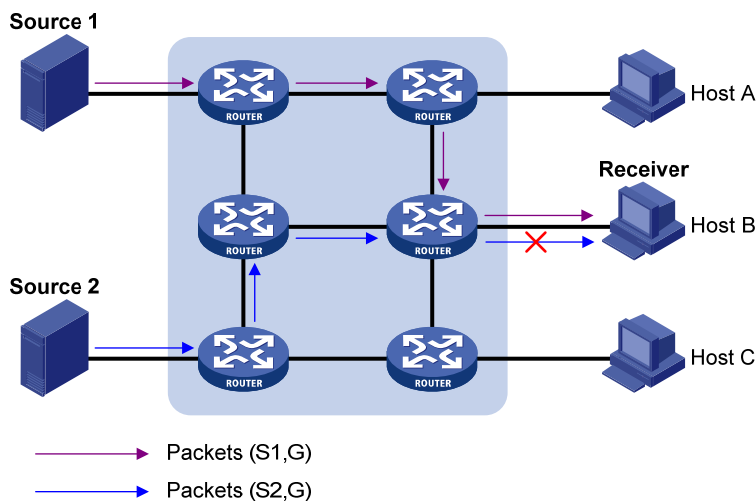
Enhancements in control capability of hosts

IGMPv3 introduced two source filtering modes—Include and Exclude. These modes allow a host to join a designated multicast group and to choose whether to receive or reject multicast data from designated multicast sources. When a host joins a multicast group, one of the following situation occurs:

- If it needs to receive multicast data from specific sources like S1, S2, ..., it sends a report with the Filter-Mode denoted as "Include Sources (S1, S2, ...)."
- If it needs to reject multicast data from specific sources like S1, S2, ..., it sends a report with the Filter-Mode denoted as "Exclude Sources (S1, S2, ...)."

As shown in [Figure 34](#), the network comprises two multicast sources, Source 1 (S1) and Source 2 (S2), both of which can send multicast data to multicast group G. Host B is only interested in the multicast data that Source 1 sends to G but not in the data from Source 2.

Figure 34 Flow paths of source-and-group-specific multicast traffic



In the case of IGMPv1 or IGMPv2, Host B cannot select multicast sources when it joins multicast group G. Therefore, multicast streams from both Source 1 and Source 2 will flow to Host B whether or not it needs them.

When IGMPv3 is running between the hosts and routers, Host B can explicitly express that it needs to receive the multicast data that Source 1 sends to multicast group G—denoted as (S1, G), rather than the

multicast data that Source 2 sends to multicast group G —denoted as $(S2, G)$. Thus, only multicast data from Source 1 will be delivered to Host B.

Enhancements in query and report capabilities

1. Query message carrying the source addresses

IGMPv3 supports not only general queries (feature of IGMPv1) and group-specific queries (feature of IGMPv2), but also group-and-source-specific queries.

- A general query does not carry a group address or a source address.
- A group-specific query carries a group address, but no source address.
- A group-and-source-specific query carries a group address and one or more source addresses.

2. Reports containing multiple group records

Unlike an IGMPv1 or IGMPv2 report message, an IGMPv3 report message is destined to 224.0.0.22 and contains one or more group records. Each group record contains a multicast group address and a multicast source address list.

Group records fall into the following categories:

- **IS_IN**—The source filtering mode is Include. The report sender requests the multicast data from only the sources defined in the specified multicast source list.
- **IS_EX**—The source filtering mode is Exclude. The report sender requests the multicast data from any sources but those defined in the specified multicast source list.
- **TO_IN**—The filtering mode has changed from Exclude to Include.
- **TO_EX**—The filtering mode has changed from Include to Exclude.
- **ALLOW**—The Source Address fields in this group record contain a list of the additional sources that the system wants to obtain data from, for packets sent to the specified multicast address. If the change was to an Include source list, these sources are the addresses that were added to the list. If the change was to an Exclude source list, these sources are the addresses that were deleted from the list.
- **BLOCK**—The Source Address fields in this group record contain a list of the sources that the system no longer wants to obtain data from, for packets sent to the specified multicast address. If the change was to an Include source list, these sources are the addresses that were deleted from the list. If the change was to an Exclude source list, these sources are the addresses that were added to the list.

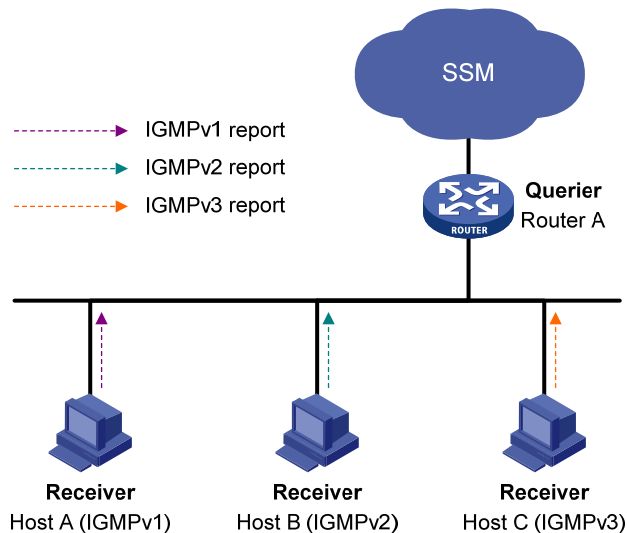
IGMP SSM mapping

The IGMP SSM mapping feature enables you to configure static IGMP SSM mappings on the last-hop router to provide SSM support for receiver hosts that are running IGMPv1 or IGMPv2. The SSM model assumes that the last-hop router has identified the desired multicast sources when receivers join multicast groups.

- When a host that is running IGMPv3 joins a multicast group, it can explicitly specify one or more multicast sources in its IGMPv3 report.

- A host that is running IGMPv1 or IGMPv2, however, cannot specify multicast source addresses in its report. In this case, you must configure the IGMP SSM mapping feature to translate the (*, G) information in the IGMPv1 or IGMPv2 report into (G, INCLUDE, (S1, S2...)) information.

Figure 35 Network diagram



As shown in [Figure 35](#), on an SSM network, Host A, Host B, and Host C are running IGMPv1, IGMPv2, and IGMPv3 respectively. To provide SSM service for all the hosts if IGMPv3 is not available on Host A and Host B, you must configure the IGMP SSM mapping feature on Router A.

With the IGMP SSM mapping feature configured, when Router A receives an IGMPv1 or IGMPv2 report, it checks the multicast group address G carried in the message and does the following:

- If G is not in the SSM group range, Router A cannot provide the SSM service but can provide the ASM service.
- If G is in the SSM group range but no IGMP SSM mappings that correspond to the multicast group G have been configured on Router A, Router A cannot provide SSM service and drops the message.
- If G is in the SSM group range and the IGMP SSM mappings have been configured on Router A for multicast group G, Router A translates the (*, G) information in the IGMP report into (G, INCLUDE, (S1, S2...)) information based on the configured IGMP SSM mappings and provides SSM service accordingly.

NOTE:

The IGMP SSM mapping feature does not process IGMPv3 reports.

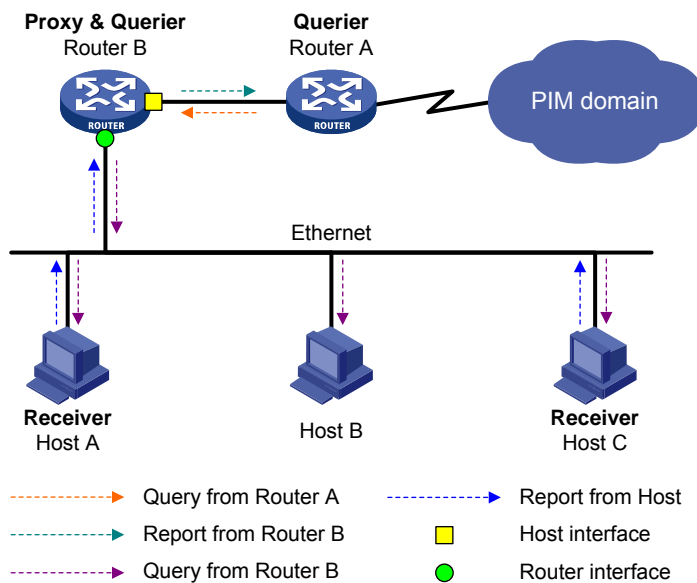
For more information about the SSM group range, see "[Configuring PIM \(available only on the HP 5500 EI\).](#)"

IGMP proxying

In some simple tree-shaped topologies, it is not necessary to configure complex multicast routing protocols, such as PIM, on the boundary devices. Instead, you can configure IGMP proxying on these

devices. With IGMP proxying configured, the device serves as a proxy for the downstream hosts to send IGMP messages, maintain group memberships, and implement multicast forwarding based on the memberships. In this case, each boundary device is a host but no longer a PIM neighbor to the upstream device.

Figure 36 Network diagram



As shown in [Figure 36](#), the following types of interfaces are defined on an IGMP proxy device:

- **Upstream interface**—Also called the "proxy interface". A proxy interface is an interface on which IGMP proxying is configured. It is in the direction toward the root of the multicast forwarding tree. An upstream interface acts as a host that is running IGMP. Therefore, it is also called the "host interface".
- **Downstream interface**—An interface that is running IGMP and is not in the direction toward the root of the multicast forwarding tree. A downstream interface acts as a router that is running IGMP. Therefore, it is also called the "router interface".

A device with IGMP proxying configured maintains a group membership database, which stores the group memberships on all the downstream interfaces. Each entry comprises the multicast address, filter mode, and source list. Such an entry is a collection of members in the same multicast group on each downstream interface.

A proxy device performs host functions on the upstream interface based on the database. It responds to queries according to the information in the database or sends join/leave messages when the database changes. On the other hand, the proxy device performs router functions on the downstream interfaces by participating in the querier election, sending queries, and maintaining memberships based on the reports.

IGMP support for VPNs

IGMP maintains group memberships on a per-interface base. After receiving an IGMP message on an interface, IGMP processes the packet within the VPN that the interface belongs to. If IGMP that runs in a VPN needs to exchange information with another multicast protocol, it passes the information only to the protocol that runs in this VPN.

Protocols and standards

- RFC 1112, *Host Extensions for IP Multicasting*
- RFC 2236, *Internet Group Management Protocol, Version 2*
- RFC 3376, *Internet Group Management Protocol, Version 3*
- RFC 4605, *Internet Group Management Protocol (IGMP)/Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")*

IGMP configuration task list

Task	Remarks	
Configuring basic IGMP functions	Enabling IGMP	Required
	Configuring IGMP versions	Optional
	Configuring static joining	Optional
	Configuring a multicast group filter	Optional
	Setting the maximum number of multicast groups that an interface can join	Optional
Adjusting IGMP performance	Configuring Router-Alert option handling methods	Optional
	Configuring IGMP query and response parameters	Optional
	Configuring IGMP fast-leave processing	Optional
	Enabling the IGMP host tracking function	Optional
	Setting the DSCP value for IGMP messages	Optional
Configuring IGMP SSM mapping	Enabling SSM mapping	Optional
	Configuring SSM mappings	Optional
Configuring IGMP proxying	Enabling IGMP proxying	Optional
	Configuring multicast forwarding on a downstream interface	Optional

For the configuration tasks in this section:

- In IGMP view, the configuration is effective on all interfaces. In interface view, the configuration is effective on only the current interface.

- If a feature is not configured on an interface in interface view, the global configuration in IGMP view will apply to that interface. If a feature is configured in both IGMP view and interface view, the configuration in interface view will be given priority.

Configuring basic IGMP functions

Before you configure basic IGMP functions, complete the following tasks:

- Configure any unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Configure PIM-DM or PIM-SM.
- Determine the IGMP version.
- Determine the multicast group and multicast source addresses for static group member configuration.
- Determine the ACL rule for multicast group filtering.
- Determine the maximum number of multicast groups that an interface can join.

Enabling IGMP

To configure IGMP, you must enable IGMP on the interface for which the multicast group memberships will be established and maintained.

Enabling IGMP for the public network

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IP multicast routing.	multicast routing-enable	Disabled by default
3. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable IGMP.	igmp enable	Disabled by default

Enabling IGMP in a VPN instance

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a VPN instance and enter VPN instance view.	ip vpn-instance <i>vpn-instance-name</i>	N/A
3. Configure an RD for the VPN instance.	route-distinguisher <i>route-distinguisher</i>	No RD is configured by default.
4. Enable IP multicast routing.	multicast routing-enable	Disabled by default.
5. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A

Step	Command	Remarks
6.	Bind the interface with a VPN instance. ip binding vpn-instance <i>vpn-instance-name</i>	By default, an interface belongs to the public network, and is not bound with any VPN instance.
7.	Enable IGMP. igmp enable	Disabled by default.

For more information about the **ip vpn-instance**, **route-distinguisher**, and **ip binding vpn-instance** commands, see *IP Routing Command Reference*.

Configuring IGMP versions

Because the protocol packets of different IGMP versions vary in structure and type, you must configure the same IGMP version for all routers on the same subnet before IGMP can work properly.

Configuring an IGMP version globally

Step	Command	Remarks
1.	Enter system view. system-view	N/A
2.	Enter public network IGMP view or VPN instance IGMP view. igmp [vpn-instance <i>vpn-instance-name</i>]	N/A
3.	Configure an IGMP version globally. version <i>version-number</i>	IGMPv2 by default

Configuring an IGMP version on an interface

Step	Command	Remarks
1.	Enter system view. system-view	N/A
2.	Enter interface view. interface <i>interface-type</i> <i>interface-number</i>	N/A
3.	Configure an IGMP version on the interface. igmp version <i>version-number</i>	IGMPv2 by default

Configuring static joining

After an interface is configured as a static member of a multicast group or a multicast source group, it will act as a virtual member of the multicast group to receive multicast data addressed to that multicast group for the purpose of testing multicast data forwarding.

Configuration guidelines

- Before you can configure an interface of a PIM-SM switch as a static member of a multicast group or a multicast source and group, if the interface is PIM-SM enabled, it must be a PIM-SM DR. If the interface is enabled with IGMP but not with PIM-SM, it must be an IGMP querier. For more information about PIM-SM and DR, see "[Configuring PIM \(available only on the HP 5500 EI\)](#)"

- A static member port does not respond to queries from the IGMP querier. When you configure a port as a static member port or remove this configuration on the port, the port does not unsolicitedly send any IGMP report or IGMP leave message. In other words, the port is not a real member of the multicast group or the multicast source and group.

Configuration procedure

To configure an interface as a statically connected member of a multicast group or a multicast source and group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the interface as a static member of a multicast group or a multicast source and group.	igmp static-group <i>group-address</i> [source <i>source-address</i>]	An interface is not a static member of any multicast group or multicast source and group by default.

Configuring a multicast group filter

To restrict the hosts on the network attached to an interface from joining certain multicast groups, you can set an ACL rule on the interface as a packet filter so that the interface maintains only the multicast groups the match the criteria.

To configure a multicast group filter:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure a multicast group filter.	igmp group-policy <i>acl-number</i> [<i>version-number</i>]	By default, no multicast group filter is configured on an interface, and hosts on an interface can join any valid multicast group.

Setting the maximum number of multicast groups that an interface can join

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A

Step	Command	Remarks
3.	Configure the maximum number of multicast groups that the interface can join.	<code>igmp group-limit limit</code> 2000 by default.

NOTE:

This configuration takes effect for dynamically joined multicast groups but not for statically configured multicast groups.

Adjusting IGMP performance

For the configuration tasks described in this section:

- The configuration in IGMP view is effective on all interfaces, whereas the configuration in interface view is effective only on the current interface.
- If the same feature is configured in both IGMP view and interface view, the configuration in interface view is given priority, regardless of the configuration sequence.

Configuration prerequisites

Before adjusting IGMP performance, complete the following tasks:

- Configure any unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Configure basic IGMP functions.
- Determine the startup query interval.
- Determine the startup query count.
- Determine the IGMP general query interval.
- Determine the IGMP querier's robustness variable.
- Determine the maximum response time for IGMP general queries.
- Determine the IGMP last-member query interval.
- Determine the other querier present interval.
- Determine the DSCP value for IGMP messages.

Configuring Router-Alert option handling methods

IGMP queries include group-specific queries and group-and-source-specific queries, and multicast groups change dynamically, so a device cannot maintain the information for all multicast sources and groups. For this reason, when an IGMP router receives a multicast packet but cannot locate the outgoing interface for the destination multicast group, it must use the Router-Alert option to pass the multicast packet to the upper-layer protocol for processing. For more information about the Router-Alert option, see RFC 2113.

An IGMP message is processed differently depending on whether it carries the Router-Alert option in the IP header:

- By default, for the consideration of compatibility, the switch does not verify the Router-Alert option but processes all the IGMP messages that it received. In this case, IGMP messages are directly passed to the upper-layer protocol, whether or not the IGMP messages carry the Router-Alert option.
- To enhance the switch performance and avoid unnecessary costs, and also for the consideration of protocol security, you can configure the switch to discard IGMP messages that do not carry the Router-Alert option.

Configuring Router-Alert option handling methods globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network IGMP view or VPN instance IGMP view.	igmp [vpn-instance vpn-instance-name]	N/A
3. Configure the router to discard any IGMP message that does not carry the Router-Alert option.	require-router-alert	By default, the switch does not check the Router-Alert option.
4. Enable insertion of the Router-Alert option into IGMP messages.	send-router-alert	By default, IGMP messages carry the Router-Alert option.

Configuring Router-Alert option handling methods on an interface

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface interface-type interface-number	N/A
3. Configure the interface to discard any IGMP message that does not carry the Router-Alert option.	igmp require-router-alert	By default, the switch does not check the Router-Alert option.
4. Enable insertion of the Router-Alert option into IGMP messages.	igmp send-router-alert	By default, IGMP messages carry the Router-Alert option.

Configuring IGMP query and response parameters

On startup, the IGMP querier sends IGMP general queries at the startup query interval, which is one-quarter of the IGMP general query interval. The number of queries, or the startup query count, is user configurable.

After startup, the IGMP querier periodically sends IGMP general queries at the IGMP general query interval to check for multicast group members on the network. You can modify the IGMP general query interval based on actual condition of the network.

The IGMPv2 querier sends IGMP group-specific queries at the IGMP last-member query interval when it receives an IGMP leave message. The IGMPv3 querier sends IGMP group-and-source-specific queries at the IGMP last-member query interval when it receives a multicast group and multicast mapping change report. The number of queries, or the last-member query count, equals the robustness variable—the maximum number of packet retransmissions.

A multicast listening host starts a delay timer for each multicast group it has joined when it receives an IGMP query (general query, group-specific query, or group-and-source-specific query). The timer is initialized to a random value in the range of 0 to the maximum response time derived in the IGMP query. When the timer value decreases to 0, the host sends an IGMP report to the corresponding multicast group.

To speed up the response of hosts to IGMP queries and avoid simultaneous timer expirations causing IGMP report traffic bursts, you must properly set the maximum response time.

- For IGMP general queries, the maximum response time is set by the **max-response-time** command.
- For IGMP group-specific queries and IGMP group-and-source-specific queries, the maximum response time equals the IGMP last-member query interval.

When multiple multicast routers exist on the same subnet, the IGMP querier is responsible for sending IGMP queries. If a non-querier router receives no IGMP query from the querier when the other querier present interval expires, it considers that the querier as having failed and starts a new querier election. Otherwise, the non-querier router resets the other querier present timer.

Configuration guidelines

- In the configuration, make sure that the other querier present interval is greater than the IGMP general query interval. Otherwise, the IGMP querier might change frequently on the network.
- Also make sure that the IGMP general query interval is greater than the maximum response time for IGMP general queries. Otherwise, multicast group members might be wrongly removed.
- The configurations of the maximum response time for IGMP general queries, the IGMP last-member query interval and the IGMP other querier present interval are effective only for IGMPv2 and IGMPv3.

Configuration procedure

To configure IGMP query and response parameters globally:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network IGMP view or VPN instance IGMP view.	igmp [vpn-instance vpn-instance-name]	N/A
3. Configure the IGMP querier's robustness variable.	robust-count robust-value	2 by default.

Step	Command	Remarks
4. Configure the startup query interval.	startup-query-interval <i>interval</i>	By default, the startup query interval is 1/4 of the "IGMP general query interval."
5. Configure the startup query count.	startup-query-count <i>value</i>	By default, the startup query count is set to the IGMP querier's robustness variable.
6. Configure the IGMP general query interval.	timer query <i>interval</i>	60 seconds by default.
7. Configure the maximum response time for IGMP general queries.	max-response-time <i>interval</i>	10 seconds by default.
8. Configure the IGMP last-member query interval.	last-member-query-interval <i>interval</i>	1 second by default.
9. Configure the other querier present interval.	timer other-querier-present <i>interval</i>	By default, the other querier present interval is [IGMP general query interval] × [IGMP robustness variable] + [maximum response time for IGMP general queries] / 2.

To configure IGMP query and response parameters on an interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the IGMP querier's robustness variable.	igmp robust-count <i>robust-value</i>	2 by default.
4. Configure the startup query interval.	igmp startup-query-interval <i>interval</i>	By default, the startup query interval is 1/4 of the "IGMP general query interval."
5. Configure the startup query count.	igmp startup-query-count <i>value</i>	By default, the startup query count is set to the IGMP querier's robustness variable.
6. Configure the IGMP general query interval.	igmp timer query <i>interval</i>	60 seconds by default.
7. Configure the maximum response time for IGMP general queries.	igmp max-response-time <i>interval</i>	10 seconds by default.
8. Configure the IGMP last-member query interval.	igmp last-member-query-interval <i>interval</i>	1 second by default
9. Configure the other querier present interval.	igmp timer other-querier-present <i>interval</i>	By default, the other querier present interval is [IGMP general query interval] × [IGMP robustness variable] + [maximum response time for IGMP general queries] / 2.

Configuring IGMP fast-leave processing

In some applications, such as ADSL dial-up networking, only one multicast receiver host is attached to a port of the IGMP querier. To allow fast response to the leave messages of the host when it switches frequently from one multicast group to another, you can enable IGMP fast-leave processing on the IGMP querier.

With IGMP fast-leave processing enabled, after receiving an IGMP leave message from a host, the IGMP querier directly sends a leave notification to the upstream without sending IGMP group-specific queries or IGMP group-and-source-specific queries. Thus, the leave latency is reduced on one hand, and the network bandwidth is saved on the other hand.

Configuration guidelines

- The IGMP fast-leave processing configuration is effective only if the switch is running IGMPv2 or IGMPv3.
- The IGMP fast-leave processing configuration is effective on Layer 3 interfaces other than VLAN interfaces, including Layer 3 Ethernet ports, Layer 3 aggregate interfaces, and Tunnel interfaces.

Configuration procedure

To configure IGMP fast-leave processing globally:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network IGMP view or VPN instance IGMP view.	igmp [vpn-instance vpn-instance-name]	N/A
3. Configure IGMP fast-leave processing.	fast-leave [group-policy acl-number]	Disabled by default

To configure IGMP fast-leave processing on an interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface interface-type interface-number	N/A
3. Configure IGMP fast-leave processing.	igmp fast-leave [group-policy acl-number]	Disabled by default

IGMP fast-leave processing is implemented by IGMP snooping. For more information, see "[Configuring IGMP snooping](#)."

Enabling the IGMP host tracking function

With the IGMP host tracking function, the switch can record the information of the member hosts that are receiving multicast traffic, including the host IP address, running duration, and timeout time. You can monitor and manage the member hosts according to the recorded information.

Enabling the IGMP host tracking function globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network IGMP view/VPN instance IGMP view.	igmp [vpn-instance vpn-instance-name]	N/A
3. Enable the IGMP host tracking function globally.	host-tracking	Disabled by default

Enabling the IGMP host tracking function on an interface

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface interface-type interface-number	N/A
3. Enable the IGMP host tracking function on the interface.	igmp host-tracking	Disabled by default

Setting the DSCP value for IGMP messages

IPv4 uses an eight-bit ToS field to identify type of service for IP packets. As defined in RFC 2474, the first six bits contains the DSCP priority for prioritizing traffic in the network and the last two bits are reserved.

To set the DSCP value for IGMP messages:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network IGMP view or VPN instance IGMP view.	igmp [vpn-instance vpn-instance-name]	N/A
3. Set the DSCP value for IGMP messages.	dscp dscp-value	Optional. By default, the DSCP value in IGMP messages is 48.

Configuring IGMP SSM mapping

Because of some possible restrictions, some receiver hosts on an SSM network might run IGMPv1 or IGMPv2. To provide SSM service support for these receiver hosts, configure the IGMP mapping feature on the last-hop router.

Before you configure the IGMP SSM mapping feature, complete the following tasks:

- Configure any unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Configure basic IGMP functions.

Enabling SSM mapping

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable the IGMP SSM mapping feature.	igmp ssm-mapping enable	Disabled by default

NOTE:

To ensure SSM service for all hosts on a subnet, regardless of the IGMP version running on the hosts, enable IGMPv3 on the interface that forwards multicast traffic onto the subnet.

Configuring SSM mappings

By performing this configuration multiple times, you can map a multicast group to different multicast sources.

If IGMPv3 is enabled on a VLAN interface of a switch, and if a port in that VLAN is configured as a simulated host, the simulated host will send IGMPv3 reports even if you did not specify a multicast source when you configure simulated joining with the **igmp-snooping host-join** command. In this case, the corresponding multicast group will not be created based on the configured IGMP SSM mappings. For more information about the **igmp-snooping host-join** command, see *IP Multicast Command Reference*.

To configure an IGMP SSM mapping:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network IGMP view or VPN instance IGMP view.	igmp [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Configure an IGMP SSM mapping.	ssm-mapping <i>group-address</i> { <i>mask</i> <i>mask-length</i> } <i>source-address</i>	No IGMP mappings are configured by default.

Configuring IGMP proxying

Before you configure the IGMP proxying feature, complete the following tasks:

- Configure any unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Enable IP multicast routing.

Enabling IGMP proxying

You can enable IGMP proxying on the interface in the direction toward the root of the multicast forwarding tree to make the switch serve as an IGMP proxy.

Configuration guidelines

- Each switch can have only one interface serving as the proxy interface. In scenarios with multiple instances, IGMP proxying is configured on only one interface per instance.
- You cannot enable IGMP on an interface with IGMP proxying enabled. Moreover, only the **igmp require-router-alert**, **igmp send-router-alert**, and **igmp version** commands can take effect on such an interface.
- You cannot enable other multicast routing protocols (such as PIM-DM or PIM-SM) on an interface with IGMP proxying enabled, or vice versa. However, the **source-lifetime**, **source-policy**, and **ssm-policy** commands configured in PIM view can still take effect. In addition, in IGMPv1, the designated router (DR) is elected by the working multicast routing protocol (such as PIM) to serve as the IGMP querier. Therefore, a downstream interface running IGMPv1 cannot be elected as the DR and thus cannot serve as the IGMP querier.
- You cannot enable IGMP proxying on a VLAN interface with IGMP snooping enabled, or vice versa.

Configuration procedure

To enable IGMP proxying:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable the IGMP proxying feature.	igmp proxying enable	Disabled by default

Configuring multicast forwarding on a downstream interface

Only queriers can forward multicast traffic but non-queriers have no multicast forwarding capabilities. This design helps avoid duplicate multicast flows. It is the same on IGMP proxy switches. Only the downstream interfaces acting as a querier can forward multicast traffic to downstream hosts.

However, when a downstream interface of a proxy switch fails to win the querier election, you must enable multicast forwarding on this interface.

On a multi-access network with more than one IGMP proxy switch, you cannot enable multicast forwarding on any other non-querier downstream interface after one of the downstream interfaces of these IGMP proxy switches has been elected as the querier. Otherwise, duplicate multicast flows might be received on the multi-access network.

To enable multicast forwarding on a downstream interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable multicast forwarding on a non-querier downstream interface.	igmp proxying forwarding	Disabled by default

Displaying and maintaining IGMP

⚠ CAUTION:

The **reset igmp group** command might cause multicast data transmission failures.

To display and maintain IGMP:

Task	Command	
Display IGMP group information.	display igmp [all-instance vpn-instance <i>vpn-instance-name</i>] group [<i>group-address</i> interface <i>interface-type interface-number</i>] [static verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the Layer 2 port information of IGMP groups.	display igmp group port-info [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

Task	Command	
Display information about the hosts tracked by IGMP on an interface.	display igmp host interface <i>interface-type interface-number</i> group <i>group-address</i> [source <i>source-address</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display information about the hosts tracked by IGMP on the Layer 2 ports.	display igmp host port-info vlan <i>vlan-id</i> group <i>group-address</i> [source <i>source-address</i>] [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display IGMP configuration and operation information.	display igmp [all-instance vpn-instance <i>vpn-instance-name</i>] interface [<i>interface-type interface-number</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the information of IGMP proxying groups.	display igmp [all-instance vpn-instance <i>vpn-instance-name</i>] proxying group [<i>group-address</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display information in the IGMP routing table.	display igmp [all-instance vpn-instance <i>vpn-instance-name</i>] routing-table [<i>source-address</i> [mask { <i>mask</i> <i>mask-length</i> }] <i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }]] [flags { act suc }] * [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display IGMP SSM mappings.	display igmp [all-instance vpn-instance <i>vpn-instance-name</i>] ssm-mapping <i>group-address</i> [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the multicast group information created from IGMPv1 and IGMPv2 reports based on the configured IGMP SSM mappings.	display igmp [all-instance vpn-instance <i>vpn-instance-name</i>] ssm-mapping group [<i>group-address</i> interface <i>interface-type interface-number</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display information about the hosts that join the group based on IGMP SSM mappings on an interface.	display igmp ssm-mapping host interface <i>interface-type interface-number</i> group <i>group-address</i> source <i>source-address</i> [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

Task	Command	
Remove all the dynamic IGMP group entries of IGMP groups.	reset igmp [all-instance vpn-instance <i>vpn-instance-name</i>] group { all interface <i>interface-type interface-number</i> } { all <i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }] [<i>source-address</i>] } [mask { <i>mask</i> <i>mask-length</i> }] }	Available in user view. This command cannot remove static IGMP group entries.
Remove all the dynamic Layer 2 port entries of IGMP groups.	reset igmp group port-info { all <i>group-address</i> } [vlan <i>vlan-id</i>]	Available in user view.
Clear IGMP SSM mappings.	reset igmp [all-instance vpn-instance <i>vpn-instance-name</i>] ssm-mapping group { all interface <i>interface-type interface-number</i> } { all <i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }] [<i>source-address</i>] } [mask { <i>mask</i> <i>mask-length</i> }] }	Available in user view.

The **display igmp host interface** command can display information about the hosts tracked by IGMP on Layer 3 interfaces other than VLAN interfaces.

The **display igmp ssm-mapping host interface** command can display information about the hosts that join the group based on IGMP SSM mappings on Layer 3 interfaces other than VLAN interfaces.

IGMP configuration examples

Basic IGMP functions configuration example

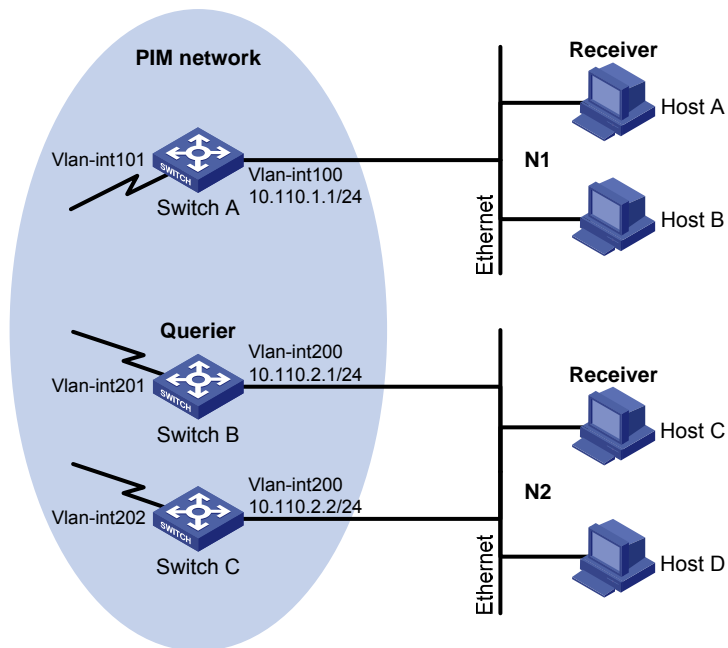
Network requirements

Receivers receive VOD information through multicast. Receivers of different organizations form stub networks N1 and N2, and Host A and Host C are receivers in N1 and N2 respectively.

IGMPv2 runs between Switch A and N1. IGMPv2 runs between the other two switches and N2. Switch B acts as the IGMP querier in N2 because it has a lower IP address.

The hosts in N1 can join only multicast group 224.1.1.1, and the hosts in N2 can join any multicast groups.

Figure 37 Network diagram



Configuration procedure

1. Configure the IP address and subnet mask of each interface as per [Figure 37](#). (Details not shown.)
2. Configure OSPF on the switches in the PIM network to make sure the switches are interoperable at the network layer and they can dynamically update their routing information. (Details not shown.)
3. Enable IP multicast routing, and enable PIM-DM and IGMP:

Enable IP multicast routing on Switch A, enable PIM-DM on each interface, and enable IGMP on VLAN-interface 100.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim dm
[SwitchA-Vlan-interface101] quit
```

Enable IP multicast routing on Switch B, enable PIM-DM on each interface, and enable IGMP on VLAN-interface 200.

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
[SwitchB-Vlan-interface200] pim dm
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 201
```

```
[SwitchB-Vlan-interface201] pim dm
[SwitchB-Vlan-interface201] quit
```

Enable IP multicast routing on Switch C, enable PIM-DM on each interface, and enable IGMP on VLAN-interface 200.

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] igmp enable
[SwitchC-Vlan-interface200] pim dm
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] pim dm
[SwitchC-Vlan-interface202] quit
```

4. Configure a multicast group filter on Switch A, so that the hosts connected to VLAN-interface 100 can join only multicast group 224.1.1.1.

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 224.1.1.1 0
[SwitchA-acl-basic-2001] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp group-policy 2001
[SwitchA-Vlan-interface100] quit
```

Verifying the configuration

Display IGMP information on VLAN-interface 200 of Switch B.

```
[SwitchB] display igmp interface vlan-interface 200
Vlan-interface200(10.110.2.1):
  IGMP is enabled
  Current IGMP version is 2
  Value of query interval for IGMP(in seconds): 60
  Value of other querier present interval for IGMP(in seconds): 125
  Value of maximum query response time for IGMP(in seconds): 10
  Querier for IGMP: 10.110.2.1 (this router)
Total 1 IGMP Group reported
```

SSM mapping configuration example

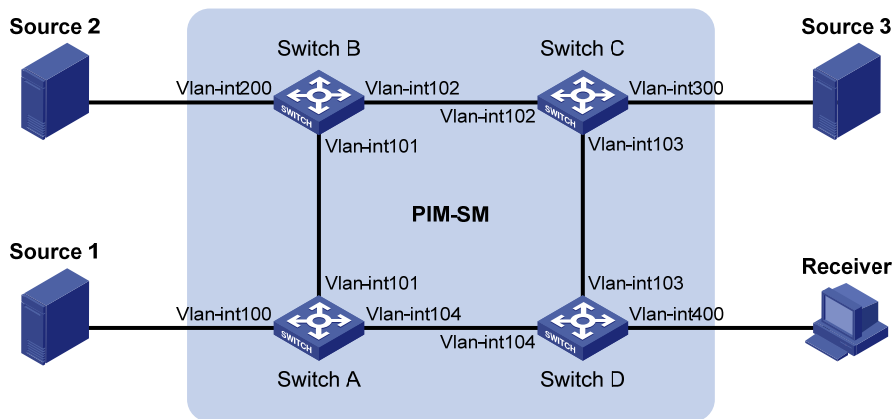
Network requirements

The PIM-SM domain applies both the ASM model and SSM model for multicast delivery. Switch D's VLAN-interface 104 serves as the C-BSR and C-RP. The SSM group range is 232.1.1.0/24.

IGMPv3 runs on Switch D's VLAN-interface 400. The receiver host runs IGMPv2, and does not support IGMPv3. Therefore, the Receiver host cannot specify expected multicast sources in its membership reports.

Source 1, Source 2, and Source 3 send multicast packets to multicast groups in the SSM group range. You can configure the IGMP SSM mapping feature on Switch D so that the receiver host will receive multicast data from Source 1 and Source 3 only.

Figure 38 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Source 1	—	133.133.1.1/24	Source 3	—	133.133.3.1/24
Source 2	—	133.133.2.1/24	Receiver	—	133.133.4.1/24
Switch A	Vlan-int100	133.133.1.2/24	Switch C	Vlan-int300	133.133.3.2/24
	Vlan-int101	192.168.1.1/24		Vlan-int103	192.168.3.1/24
	Vlan-int104	192.168.4.2/24		Vlan-int102	192.168.2.2/24
Switch B	Vlan-int200	133.133.2.2/24	Switch D	Vlan-int400	133.133.4.2/24
	Vlan-int101	192.168.1.2/24		Vlan-int103	192.168.3.2/24
	Vlan-int102	192.168.2.1/24		Vlan-int104	192.168.4.1/24

Configuration procedure

1. Configure the IP address and subnet mask of each interface as per Figure 38. (Details not shown.)
2. Configure OSPF on the switches in the PIM-SM domain to make sure the switches are interoperable at the network layer and they can dynamically update their routing information. (Details not shown.)
3. Enable IP multicast routing, enable PIM-SM on each interface, and enable IGMP and IGMP SSM mapping on the host-side interface:

Enable IP multicast routing on Switch D, enable PIM-SM on each interface, and enable IGMPv3 and IGMP SSM mapping on VLAN-interface 400.

```

<SwitchD> system-view
[SwitchD] multicast routing-enable
[SwitchD] interface vlan-interface 400
[SwitchD-Vlan-interface400] igmp enable
[SwitchD-Vlan-interface400] igmp version 3
[SwitchD-Vlan-interface400] igmp ssm-mapping enable
[SwitchD-Vlan-interface400] pim sm
[SwitchD-Vlan-interface400] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim sm
[SwitchD-Vlan-interface103] quit
[SwitchD] interface vlan-interface 104

```

```
[SwitchD-Vlan-interface104] pim sm
[SwitchD-Vlan-interface104] quit
```

Enable IP multicast routing on Switch A, and enable PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 104
[SwitchA-Vlan-interface104] pim sm
[SwitchA-Vlan-interface104] quit
```

Enable IP multicast routing and PIM-SM on Switch B and Switch C in the same way. (Details not shown.)

4. Configure C-BSR and C-RP interfaces on Switch D.

```
[SwitchD] pim
[SwitchD-pim] c-bsr vlan-interface 104
[SwitchD-pim] c-rp vlan-interface 104
[SwitchD-pim] quit
```

5. Configure the SSM group range:

Configure the SSM group range 232.1.1.0/24 on Switch D.

```
[SwitchD] acl number 2000
[SwitchD-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[SwitchD-acl-basic-2000] quit
[SwitchD] pim
[SwitchD-pim] ssm-policy 2000
[SwitchD-pim] quit
```

Configure the SSM group range 232.1.1.0/24 on Switch A, Switch B and Switch C in the same way. (Details not shown.)

6. Configure IGMP SSM mappings on Switch D.

```
[SwitchD] igmp
[SwitchD-igmp] ssm-mapping 232.1.1.0 24 133.133.1.1
[SwitchD-igmp] ssm-mapping 232.1.1.0 24 133.133.3.1
[SwitchD-igmp] quit
```

Verifying the configuration

Display the IGMP SSM mapping information for multicast group 232.1.1.1 on Switch D.

```
[SwitchD] display igmp ssm-mapping 232.1.1.1
Vpn-Instance: public net
Group: 232.1.1.1
Source list:
    133.133.1.1
    133.133.3.1
```

Display the IGMP group information created based on the IGMP SSM mappings on Switch D.

```
[SwitchD] display igmp ssm-mapping group
Total 1 IGMP SSM-mapping Group(s).
Interface group report information of VPN-Instance: public net
Vlan-interface400(133.133.4.2):
  Total 1 IGMP SSM-mapping Group reported
  Group Address      Last Reporter    Uptime          Expires
  232.1.1.1         133.133.4.1    00:02:04       off
```

Display PIM routing table information on Switch D.

```
[SwitchD] display pim routing-table
Vpn-instance: public net
Total 0 (*, G) entry; 2 (S, G) entry

(133.133.1.1, 232.1.1.1)
  Protocol: pim-ssm, Flag:
  UpTime: 00:13:25
  Upstream interface: Vlan-interface104
    Upstream neighbor: 192.168.4.2
    RPF prime neighbor: 192.168.4.2
  Downstream interface(s) information:
    Total number of downstreams: 1
    1: Vlan-interface400
      Protocol: igmp, UpTime: 00:13:25, Expires: -

(133.133.3.1, 232.1.1.1)
  Protocol: pim-ssm, Flag:
  UpTime: 00:13:25
  Upstream interface: Vlan-interface103
    Upstream neighbor: 192.168.3.1
    RPF prime neighbor: 192.168.3.1
  Downstream interface(s) information:
    Total number of downstreams: 1
    1: Vlan-interface400
      Protocol: igmp, UpTime: 00:13:25, Expires: -
```

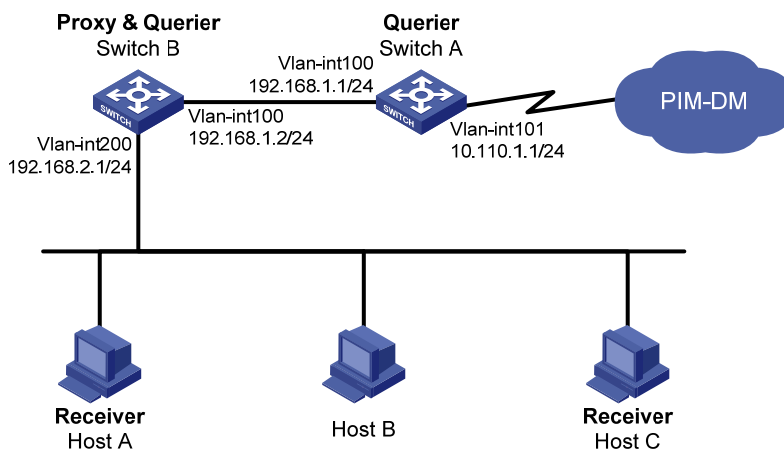
IGMP proxying configuration example

Network requirements

PIM-DM is required to run on the core network. Host A and Host C in the stub network receive VOD information destined to multicast group 224.1.1.1.

Configure the IGMP proxying feature on Switch B so that Switch B can maintain group memberships and forward multicast traffic without running PIM-DM.

Figure 39 Network diagram



Configuration procedure

1. Configure the IP address and subnet mask of each interface as per [Figure 39](#). (Details not shown.)
2. Enable IP multicast routing, PIM-DM, IGMP, and IGMP proxying:

Enable IP multicast routing on Switch A, PIM-DM on VLAN-interface 101, and IGMP on VLAN-interface 100.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim dm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
```

Enable IP multicast routing on Switch B, IGMP Proxying on VLAN-interface 100, and IGMP on VLAN-interface 200.

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp proxying enable
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
[SwitchB-Vlan-interface200] quit
```

Verifying the configuration

Display IGMP information on VLAN-interface 100 of Switch B.

```
[SwitchB] display igmp interface vlan-interface 100 verbose
Vlan-interface100(192.168.1.2):
  IGMP proxy is enabled
  Current IGMP version is 2
```

```

Multicast routing on this interface: enabled
Require-router-alert: disabled
Version1-querier-present-timer-expiry: 00:00:20

# Display IGMP group information on Switch A.
[SwitchA] display igmp group
Total 1 IGMP Group(s).
Interface group report information of VPN-Instance: public net
Vlan-interface100(192.168.1.1):
  Total 1 IGMP Groups reported
  Group Address    Last Reporter    Uptime          Expires
  224.1.1.1        192.168.1.2     00:02:04       00:01:15

```

The output shows that IGMP reports from the hosts are forwarded to Switch A through the proxy interface, VLAN-interface 100 on Switch B.

Troubleshooting IGMP

No membership information on the receiver-side router

Symptom

When a host sends a report for joining multicast group G, no membership information of the multicast group G exists on the router closest to that host.

Analysis

- The correctness of networking and interface connections and whether the protocol layer of the interface is up directly affect the generation of group membership information.
- Multicast routing must be enabled on the router, and IGMP must be enabled on the interface connecting to the host.
- If the IGMP version on the router interface is lower than that on the host, the router will not be able to recognize the IGMP report from the host.
- If the **igmp group-policy** command has been configured on the interface, the interface cannot receive report messages that fail to pass filtering.

Solution

1. Use the **display igmp interface** command to verify that the networking, interface connection, and IP address configuration are correct. If no information is output, the interface is in an abnormal state. The reason is that you have configured the **shutdown** command on the interface, the interface is not properly connected, or the IP address configuration is not correct.
2. Check that . Use the **display current-configuration** command to verify that multicast routing is enabled. If not, carry out the **multicast routing-enable** command in system view to enable IP multicast routing. In addition, check that IGMP is enabled on the corresponding interfaces.
3. Use the **display igmp interface** command to verify that the IGMP version on the interface is lower than that on the host.

4. Use the **display current-configuration interface** command to verify that no ACL rule has been configured to restrict the host from joining the multicast group G. If the host is restricted from joining the multicast group G, the ACL rule must be modified to allow receiving the reports for the multicast group G.

Inconsistent memberships on routers on the same subnet

Symptom

Different memberships are maintained on different IGMP routers on the same subnet.

Analysis

- A router running IGMP maintains multiple parameters for each interface, and these parameters influence one another, forming very complicated relationships. Inconsistent IGMP interface parameter configurations for routers on the same subnet will surely result in inconsistency of memberships.
- In addition, although an IGMP router is compatible with a host that is running a different version of IGMP, all routers on the same subnet must run the same version of IGMP. Inconsistent IGMP versions running on routers on the same subnet also leads to inconsistency of IGMP memberships.

Solution

1. Use the **display current-configuration** command to verify the IGMP configuration information on the interfaces.
2. Use the **display igmp interface** command on all routers on the same subnet to verify the IGMP-related timer settings. The settings should be consistent on all the routers.
3. Use the **display igmp interface** command to verify that all the routers on the same subnet are running the same version of IGMP.

Configuring PIM (available only on the HP 5500 EI)

PIM overview

Protocol Independent Multicast (PIM) provides IP multicast forwarding by leveraging unicast static routes or unicast routing tables generated by any unicast routing protocol, such as routing information protocol (RIP), open shortest path first (OSPF), intermediate system to intermediate system (IS-IS), or border gateway protocol (BGP). Independent of the unicast routing protocols running on the device, multicast routing can be implemented as long as the corresponding multicast routing entries are created through unicast routes. PIM uses the reverse path forwarding (RPF) mechanism to implement multicast forwarding. When a multicast packet arrives on an interface of the device, it undergoes an RPF check. If the RPF check succeeds, the device creates the corresponding routing entry and forwards the packet. If the RPF check fails, the device discards the packet. For more information about RPF, see "[Configuring multicast routing and forwarding \(available only on the HP 5500 EI\)](#)."

Based on the implementation mechanism, PIM falls into the following categories:

- Protocol Independent Multicast–Dense Mode (PIM-DM)
- Protocol Independent Multicast–Sparse Mode (PIM-SM)
- Bidirectional Protocol Independent Multicast (BIDIR-PIM)
- Protocol Independent Multicast Source-Specific Multicast (PIM-SSM)

The term "router" in this document refers to both routers and Layer 3 switches.

The term "interface" in this chapter collectively refers to Layer 3 interfaces, including VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

PIM-DM overview

PIM-DM is a type of dense mode multicast protocol. It uses the push mode for multicast forwarding, and is suitable for small-sized networks with densely distributed multicast members.

The basic implementation of PIM-DM is as follows:

- PIM-DM assumes that at least one multicast group member exists on each subnet of a network. Therefore, multicast data is flooded to all nodes on the network. Then, branches without multicast forwarding are pruned from the forwarding tree, leaving only those branches that contain receivers. This flood-and-prune process takes place periodically. Pruned branches resume multicast

forwarding when the pruned state times out. Data is then flooded again down these branches, and then the branches are pruned again.

- When a new receiver on a previously pruned branch joins a multicast group, to reduce the join latency, PIM-DM uses a graft mechanism to resume data forwarding to that branch.

Generally speaking, the multicast forwarding path is a source tree. That is, it is a forwarding tree with the multicast source as its "root" and multicast group members as its "leaves." Because the source tree is the shortest path from the multicast source to the receivers, it is also called a shortest path tree (SPT).

The working mechanism of PIM-DM is summarized as follows:

- Neighbor discovery
- SPT building
- Graft
- Assert

Neighbor discovery

In a PIM domain, a PIM router discovers PIM neighbors, maintains PIM neighboring relationships with other routers, and builds and maintains SPTs by periodically multicasting hello messages to all other PIM routers (224.0.0.13) on the local subnet.

NOTE:

Every PIM-enabled interface on a router sends hello messages periodically, and thus learns the PIM neighboring information pertinent to the interface.

SPT building

The process of building an SPT is the flood-and-prune process.

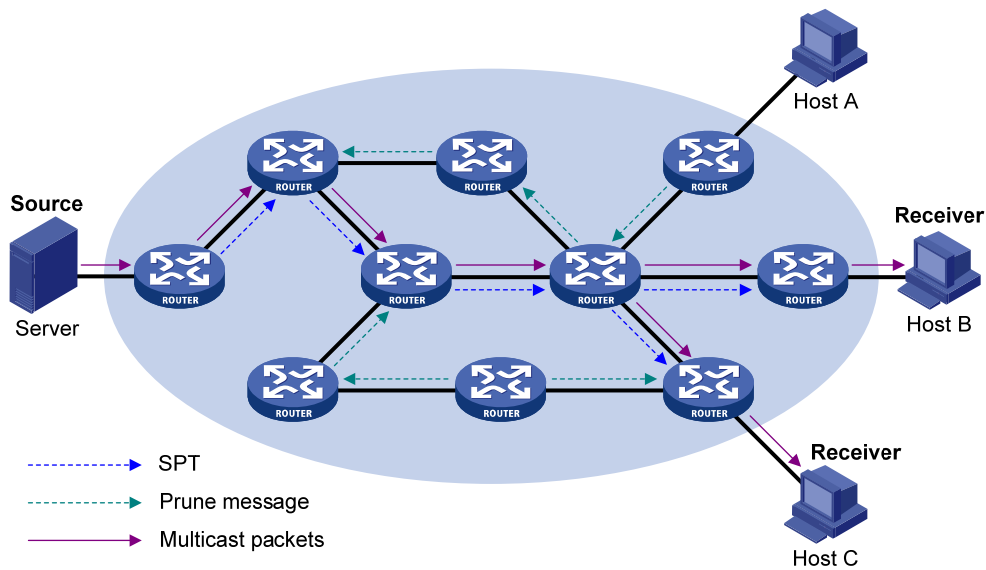
1. In a PIM-DM domain, when a multicast source *S* sends multicast data to multicast group *G*, the multicast packet is first flooded throughout the domain. The router first performs RPF check on the multicast packet. If the packet passes the RPF check, the router creates an (*S*, *G*) entry and forwards the data to all downstream nodes in the network. In the flooding process, an (*S*, *G*) entry is created on all the routers in the PIM-DM domain.
2. Then, nodes without receivers downstream are pruned. A router having no receivers downstream sends a prune message to the upstream node to "tell" the upstream node to delete the corresponding interface from the outgoing interface list in the (*S*, *G*) entry and stop forwarding subsequent packets addressed to that multicast group down to this node.

An (*S*, *G*) entry contains the multicast source address *S*, multicast group address *G*, outgoing interface list, and incoming interface.

For a given multicast stream, the interface that receives the multicast stream is referred to as "upstream," and the interfaces that forward the multicast stream are referred to as "downstream."

A prune process is first initiated by a leaf router. As shown in [Figure 40](#), a router without any receiver attached to it (the router connected with Host A, for example) sends a prune message. This prune process goes on until only necessary branches are left in the PIM-DM domain. These branches constitute the SPT.

Figure 40 SPT building



The flood-and-prune process takes place periodically. A pruned state timeout mechanism is provided. A pruned branch restarts multicast forwarding when the pruned state times out and then is pruned again when it no longer has any multicast receiver.

NOTE:

Pruning has a similar implementation in PIM-SM.

Graft

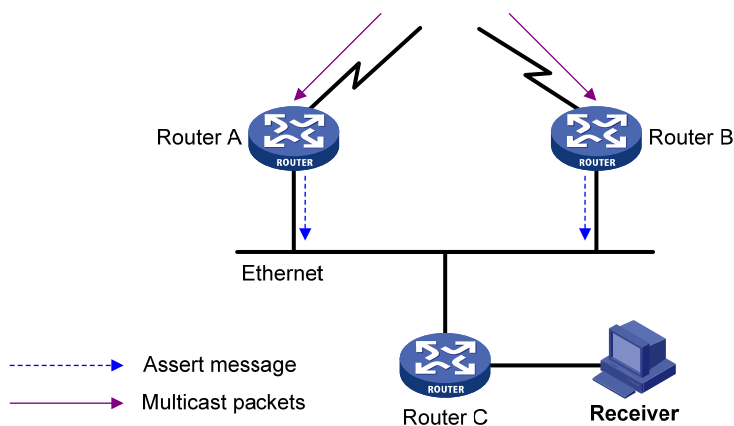
When a host attached to a pruned node joins a multicast group, to reduce the join latency, PIM-DM uses a graft mechanism to resume data forwarding to that branch. The process is as follows:

1. The node that needs to receive multicast data sends a graft message toward its upstream node as a request to join the SPT again.
2. After receiving this graft message, the upstream node puts the interface on which the graft was received into the forwarding state and responds with a graft-ack message to the graft sender.
3. If the node that sent a graft message does not receive a graft-ack message from its upstream node, it will keep sending graft messages at a configurable interval until it receives an acknowledgment from its upstream node.

Assert

Where more than one multicast router exists, the assert mechanism shuts off duplicate multicast flows onto the same multi-access network. It does this by electing a unique multicast forwarder on the multi-access network.

Figure 41 Assert mechanism



As shown in Figure 41, after Router A and Router B receive an (S, G) packet from the upstream node, they both forward the packet to the local subnet. As a result, the downstream node Router C receives two identical multicast packets, and both Router A and Router B, on their own downstream interface, receive a duplicate packet forwarded by the other. After detecting this condition, both routers send an assert message to all PIM routers (224.0.0.13) on the local subnet through the downstream interface on which the packet was received. The assert message contains the multicast source address (S), the multicast group address (G), and the preference and metric of the unicast route/MBGP route/static multicast route to the source. By comparing these parameters, either Router A or Router B becomes the unique forwarder of the subsequent (S, G) packets on the multi-access subnet. The comparison process is as follows:

1. The router with a higher preference to the source wins;
2. If both routers have the same preference to the source, the router with a smaller metric to the source wins;
3. If a tie exists in route metric to the source, the router with a higher IP address of the downstream interface wins.

PIM-SM overview

PIM-DM uses the flood-and-prune principle to build SPTs for multicast data distribution. Although an SPT has the shortest path, it is built with a low efficiency. Therefore, the PIM-DM mode is not suitable for large- and medium-sized networks.

PIM-SM is a type of sparse mode multicast protocol. It uses the pull mode for multicast forwarding and is suitable for large-sized and medium-sized networks with sparsely and widely distributed multicast group members.

The basic implementation of PIM-SM is as follows:

- PIM-SM assumes that no hosts need to receive multicast data. In the PIM-SM mode, routers must specifically request a particular multicast stream before the data is forwarded to them. The core task for PIM-SM to implement multicast forwarding will build and maintain rendezvous point trees (RPTs).

An RPT is rooted at a router in the PIM domain as the common node, or rendezvous point (RP), through which the multicast data travels along the RPT and reaches the receivers.

- When a receiver is interested in the multicast data addressed to a specific multicast group, the router connected to this receiver sends a join message to the RP that corresponds to that multicast group. The path along which the message goes hop by hop to the RP forms a branch of the RPT.
- When a multicast source sends multicast streams to a multicast group, the source-side designated router (DR) first registers the multicast source with the RP by sending register messages to the RP by unicast until it receives a register-stop message from the RP. The arrival of a register message at the RP triggers the establishment of an SPT. Then, the multicast source sends subsequent multicast packets along the SPT to the RP. After reaching the RP, the multicast packet is duplicated and delivered to the receivers along the RPT.

NOTE:

Multicast traffic is duplicated only where the distribution tree branches, and this process automatically repeats until the multicast traffic reaches the receivers.

The working mechanism of PIM-SM is summarized as follows:

- Neighbor discovery
- DR election
- RP discovery
- RPT building
- Multicast source registration
- Switchover to SPT
- Assert

Neighbor discovery

PIM-SM uses a similar neighbor discovery mechanism as PIM-DM does. For more information, see "[Neighbor discovery](#)."

DR election

PIM-SM also uses hello messages to elect a DR for a multi-access network (such as Ethernet). The elected DR will be the only multicast forwarder on this multi-access network.

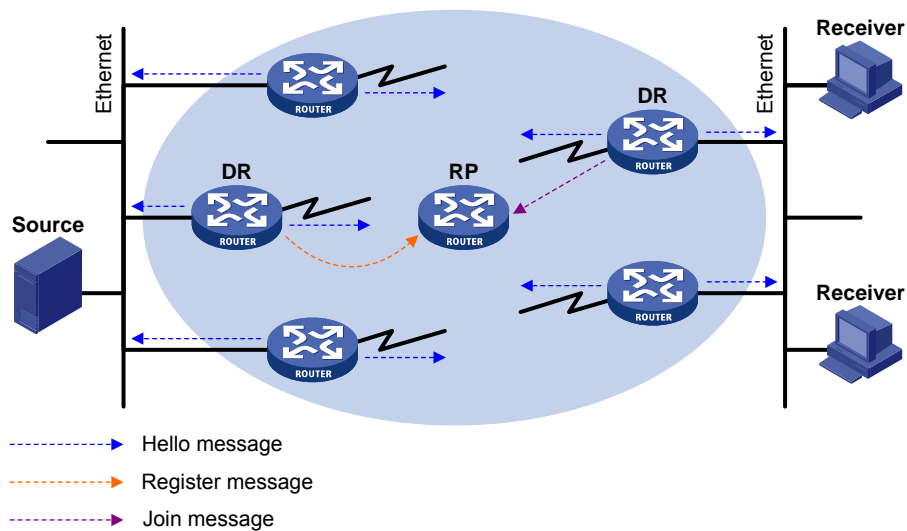
A DR must be elected in a multi-access network, no matter this network connects to multicast sources or to receivers. The receiver-side DR sends join messages to the RP. The source-side DR sends register messages to the RP.

A DR is elected on a multi-access subnet by means of comparison of the priorities and IP addresses carried in hello messages. An elected DR is substantially meaningful to PIM-SM. PIM-DM itself does not require a DR. However, if IGMPv1 runs on any multi-access network in a PIM-DM domain, a DR must be elected to act as the IGMPv1 querier on that multi-access network.

IGMP must be enabled on a device that acts as a receiver-side DR before receivers attached to this device can join multicast groups through this DR.

For more information about IGMP, see "[Configuring IGMP \(available only on the HP 5500 EI\)](#)."

Figure 42 DR election



As shown in [Figure 42](#), the DR election process is as follows:

1. Routers on the multi-access network send hello messages to one another. The hello messages contain the router priority for DR election. The router with the highest DR priority will become the DR.
2. In the case of a tie in the router priority, or if any router in the network does not support carrying the DR-election priority in hello messages, the router with the highest IP address will win the DR election.

When the DR fails, a timeout in receiving a hello message triggers a new DR election process among the other routers.

RP discovery

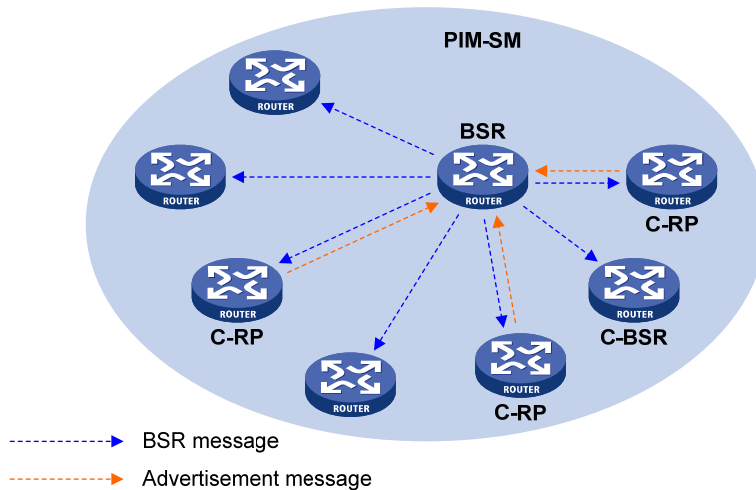
The RP is the core of a PIM-SM domain. For a small-sized, simple network, one RP is enough for forwarding information throughout the network, and you can statically specify the position of the RP on each router in the PIM-SM domain. In most cases, however, a PIM-SM network covers a wide area, and a huge amount of multicast traffic must be forwarded through the RP. To lessen the RP burden and optimize the topological structure of the RPT, you can configure multiple candidate-RPs (C-RPs) in a PIM-SM domain, among which an RP is dynamically elected through the bootstrap mechanism. Each elected RP is designated to a different multicast group range. For this purpose, you must configure a bootstrap router (BSR). The BSR acts as the administrative core of the PIM-SM domain. A PIM-SM domain can have only one BSR, but can have multiple candidate-BSRs (C-BSRs). If the BSR fails, a new BSR is automatically elected from the C-BSRs to avoid service interruption.

NOTE:

- An RP can provide services for multiple multicast groups, but a multicast group only uses one RP.
 - A device can act as a C-RP and a C-BSR at the same time.
-

As shown in Figure 43, each C-RP periodically unicasts its advertisement messages (C-RP-Adv messages) to the BSR. An advertisement message contains the address of the advertising C-RP and the multicast group range to which it is designated. The BSR collects these advertisement messages and organizes the C-RP information into an RP-set, which is a database of mappings between multicast groups and RPs. The BSR then encapsulates the RP-set in the bootstrap messages (BSMs) and floods the bootstrap messages to the entire PIM-SM domain.

Figure 43 Information exchange between C-RPs and the BSR



Based on the information in the RP-sets, all routers in the network can select the proper RP for a specific multicast group based on the following rules:

1. The C-RP that is designated to the smallest multicast group range wins.
2. If all the C-RPs are designated to the same multicast group range, the C-RP with the highest priority wins.
3. If all the C-RPs are designated to the same multicast group range and have the same priority, the C-RP with the largest hash value (calculated through the hashing algorithm) wins.
4. If all the C-RPs are designated to the same multicast group range and have the same priority and hash value, the C-RP that has the highest IP address wins.

The hashing algorithm used for RP calculation is "Value (G, M, C_i) = (1103515245 * ((1103515245 * (G & M) + 12345) XOR C_i) + 12345) mod 2³¹."

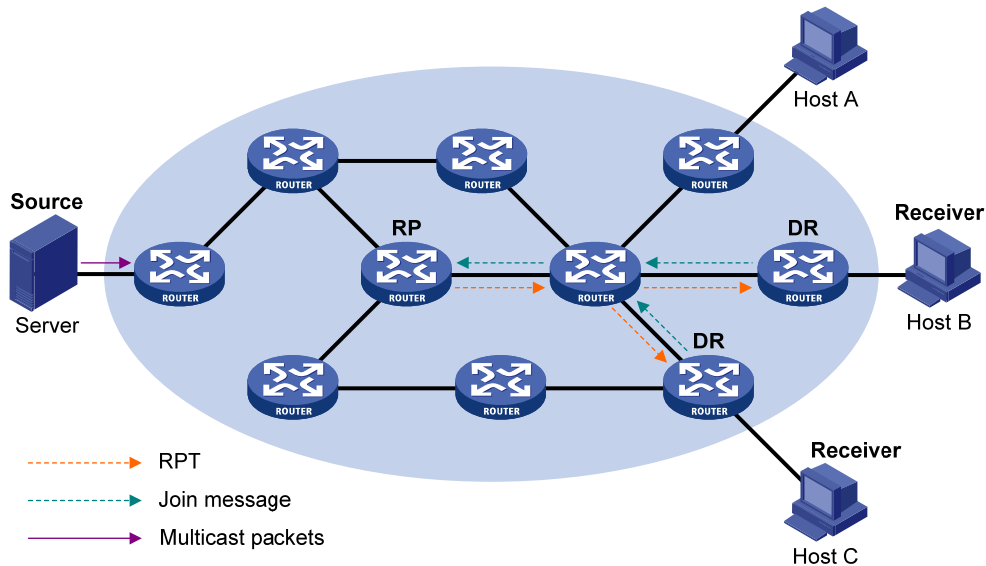
Values in the hashing algorithm

Value	Description
Value	Hash value
G	IP address of the multicast group
M	Hash mask length
C _i	IP address of the C-RP
&	Logical operator of "and"
XOR	Logical operator of "exclusive-or"

Value	Description
Mod	Modulo operator, which gives the remainder of an integer division

RPT building

Figure 44 RPT building in a PIM-SM domain



As shown in Figure 44, the process of building an RPT is as follows:

1. When a receiver joins multicast group G , it uses an IGMP message to inform the directly connected DR.
2. After getting the receiver information, the DR sends a join message, which is forwarded hop by hop to the RP that corresponds to the multicast group.
3. The routers along the path from the DR to the RP form an RPT branch. Each router on this branch generates a $(*, G)$ entry in its forwarding table. The asterisk means any multicast source. The RP is the root of the RPT, and the DRs are the leaves of the RPT.

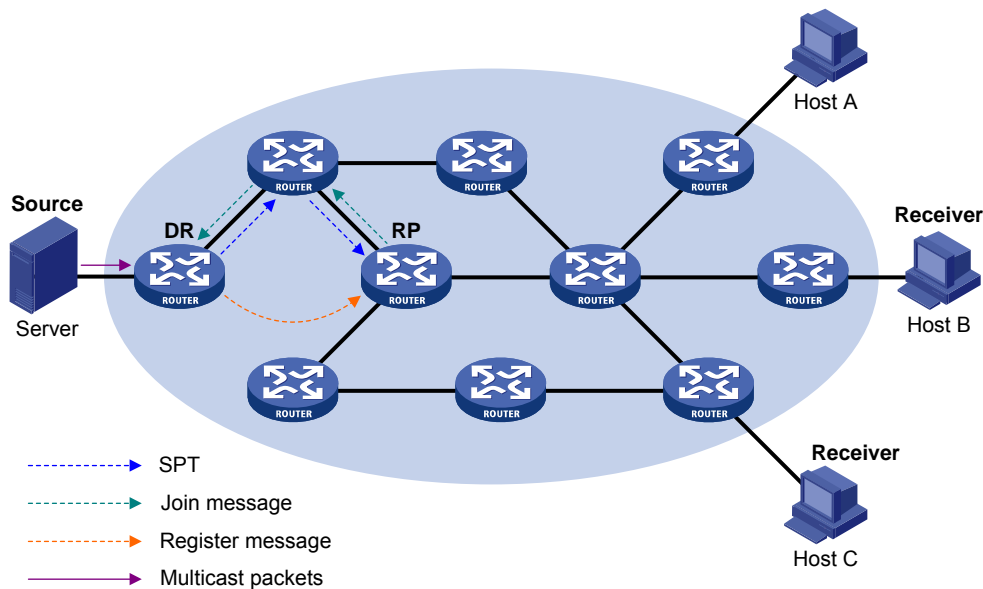
The multicast data addressed to the multicast group G flows through the RP, reaches the corresponding DR along the established RPT, and finally is delivered to the receiver.

When a receiver is no longer interested in the multicast data addressed to multicast group G , the directly connected DR sends a prune message, which goes hop by hop along the RPT to the RP. After receiving the prune message, the upstream node deletes the interface that connects to this downstream node from the outgoing interface list and determines whether it has receivers for that multicast group. If not, the router continues to forward the prune message to its upstream router.

Multicast source registration

The purpose of multicast source registration will inform the RP about the existence of the multicast source.

Figure 45 Multicast source registration



As shown in Figure 45, the multicast source registers with the RP as follows:

1. The multicast source S sends the first multicast packet to multicast group G. After receiving the multicast packet, the DR that directly connects to the multicast source encapsulates the packet in a PIM register message. Then it sends the message to the corresponding RP by unicast.
2. When the RP receives the register message, it extracts the multicast packet from the register message and forwards the multicast packet down the RPT, and sends an (S, G) join message hop by hop toward the multicast source. Thus, the routers along the path from the RP to the multicast source constitute an SPT branch. Each router on this branch generates an (S, G) entry in its forwarding table. The source-side DR is the root of the SPT, and the RP is the leaf of the SPT.
3. The subsequent multicast data from the multicast source travels along the established SPT to the RP. Then the RP forwards the data along the RPT to the receivers. When the multicast traffic arrives at the RP along the SPT, the RP sends a register-stop message to the source-side DR by unicast to stop the source registration process.

This section assumes that the RP is allowed to initiate the switchover to SPT. If the RP is not allowed to do so, the source-side DR keeps encapsulating multicast data in register messages, and the registration process will not stop unless no outgoing interfaces exist in the (S, G) entry on the RP.

Switchover to SPT

In a PIM-SM domain, a multicast group corresponds to one RP and RPT. Before the switchover to SPT occurs, the source-side DR encapsulates all multicast data destined to the multicast group in register messages and sends these messages to the RP. After receiving these register messages, the RP extracts the multicast data and sends the multicast data down the RPT to the DRs at the receiver side. The RP acts as a transfer station for all multicast packets. The whole process involves the following issues:

- The source-side DR and the RP need to implement complicated encapsulation and de-encapsulation of multicast packets.

- Multicast packets are delivered along a path that might not be the shortest one.
- An increase in multicast traffic adds a great burden on the RP, increasing the risk of failure.

To solve the issues, PIM-SM allows an RP or the DR at the receiver side to initiate the switchover to SPT.

1. The RP initiates the switchover to SPT.

The RP can periodically check the passing-by IPv4 multicast packets. If it finds that the traffic rate exceeds a configurable threshold, the RP sends an (S, G) join message hop by hop toward the multicast source to establish an SPT between the DR at the source side and the RP. Subsequent multicast data travels along the established SPT to the RP.

For more information about the switchover to SPT initiated by the RP, see "[Multicast source registration](#)."

2. The receiver-side DR initiates the switchover to SPT.

After receiving the first multicast packet, the receiver-side DR initiates the switchover to SPT, as follows:

- The receiver-side DR sends an (S, G) join message hop by hop toward the multicast source. When the join message reaches the source-side DR, all the routers on the path have installed the (S, G) entry in their forwarding table, and thus an SPT branch is established.
- When the multicast packets travel to the router where the RPT and the SPT deviate, the router drops the multicast packets received from the RPT and sends an RP-bit prune message hop by hop to the RP. After receiving this prune message, the RP sends a prune message toward the multicast source (suppose only one receiver exists). Thus, the switchover to SPT is completed.
- Multicast data is directly sent from the source to the receivers along the SPT.

PIM-SM builds SPTs through the switchover to SPT more economically than PIM-DM does through the flood-and-prune mechanism.

Assert

PIM-SM uses a similar assert mechanism as PIM-DM does. For more information, see "[Assert](#)."

BIDIR-PIM overview

In some many-to-many applications, such as multi-side video conference, there might be multiple receivers interested in multiple multicast sources simultaneously. With PIM-DM or PIM-SM, each router along the SPT must create an (S, G) entry for each multicast source, consuming a lot of system resources.

BIDIR-PIM addresses the problem. Derived from PIM-SM, BIDIR-PIM builds and maintains bidirectional RPTs, each of which is rooted at an RP and connects multiple multicast sources with multiple receivers. Traffic from the multicast sources is forwarded through the RPs to the receivers along the bidirectional RPTs. Each router needs to maintain only one (*, G) multicast routing entry, saving system resources.

BIDIR-PIM is suitable for networks with dense multicast sources and dense receivers.

The working mechanism of BIDIR-PIM is summarized as follows:

- Neighbor discovery

- RP discovery
- DF election
- Bidirectional RPT building

Neighbor discovery

BIDIR-PIM uses the same neighbor discovery mechanism as PIM-SM does. For more information, see "[Neighbor discovery](#)."

RP discovery

BIDIR-PIM uses the same RP discovery mechanism as PIM-SM does. For more information, see "[RP discovery](#)."

In PIM-SM, an RP must be specified with a real IP address. In BIDIR-PIM, however, an RP can be specified with a virtual IP address, which is called the rendezvous point address (RPA). The link corresponding to the RPA's subnet is called the rendezvous point link (RPL). All interfaces connected to the RPL can act as the RP, and they back up one another.

NOTE:

In BIDIR-PIM, an RPF interface is the interface pointing to an RP, and an RPF neighbor is the address of the next hop to the RP.

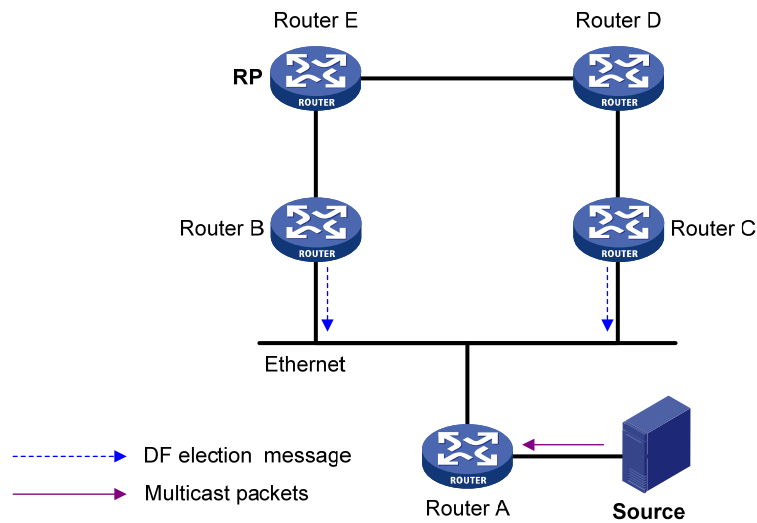
DF election

On a network segment with multiple multicast routers, the same multicast packets might be forwarded to the RP repeatedly. To address this issue, BIDIR-PIM uses a DF election mechanism to elect a unique designated forwarder (DF) for each RP on every network segment within the BIDIR-PIM domain, and allows only the DF to forward multicast data to the RP.

NOTE:

DF election is not necessary for an RPL.

Figure 46 DF election



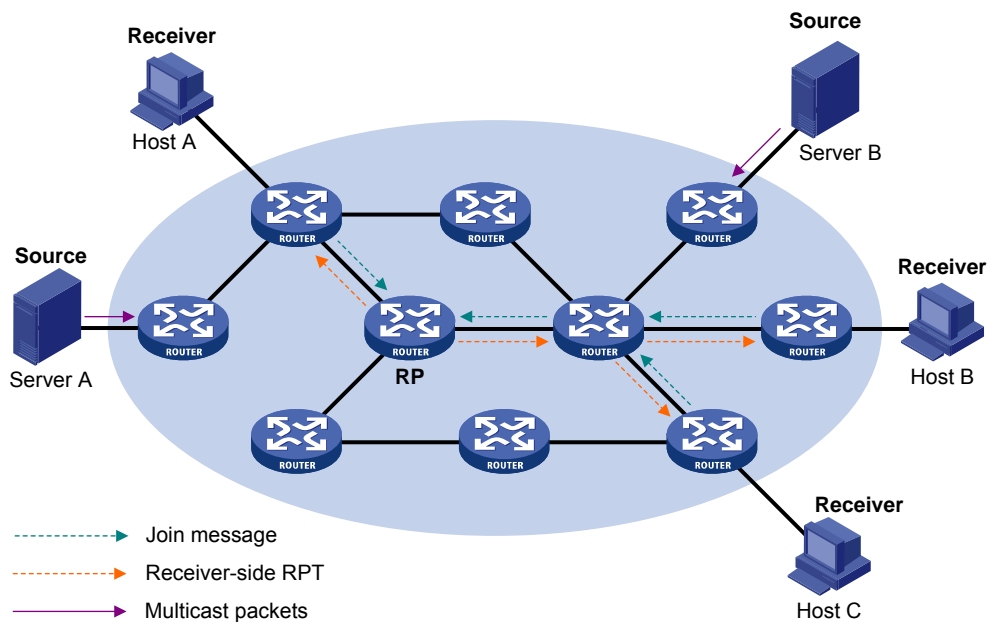
As shown in Figure 46, without the DF election mechanism, both Router B and Router C can receive multicast packets from Router A, and they might both forward the packets to downstream routers on the local subnet. As a result, the RP (Router E) receives duplicate multicast packets. With the DF election mechanism, once receiving the RP information, Router B and Router C initiate a DF election process for the RP:

1. Router B and Router C multicast DF election messages to all PIM routers (224.0.0.13). The election messages carry the RP's address, and the priority and metric of the unicast route, MBGP route, or static multicast route to the RP.
2. The router with a route of the highest priority becomes the DF.
3. In the case of a tie, the router with the route with the lowest metric wins the DF election.
4. In the case of a tie in the metric, the router with the highest IP address wins.

Bidirectional RPT building

A bidirectional RPT comprises a receiver-side RPT and a source-side RPT. The receiver-side RPT is rooted at the RP and takes the routers directly connected to the receivers as leaves. The source-side RPT is also rooted at the RP but takes the routers directly connected to the sources as leaves. The processes for building these two parts are different.

Figure 47 RPT building at the receiver side

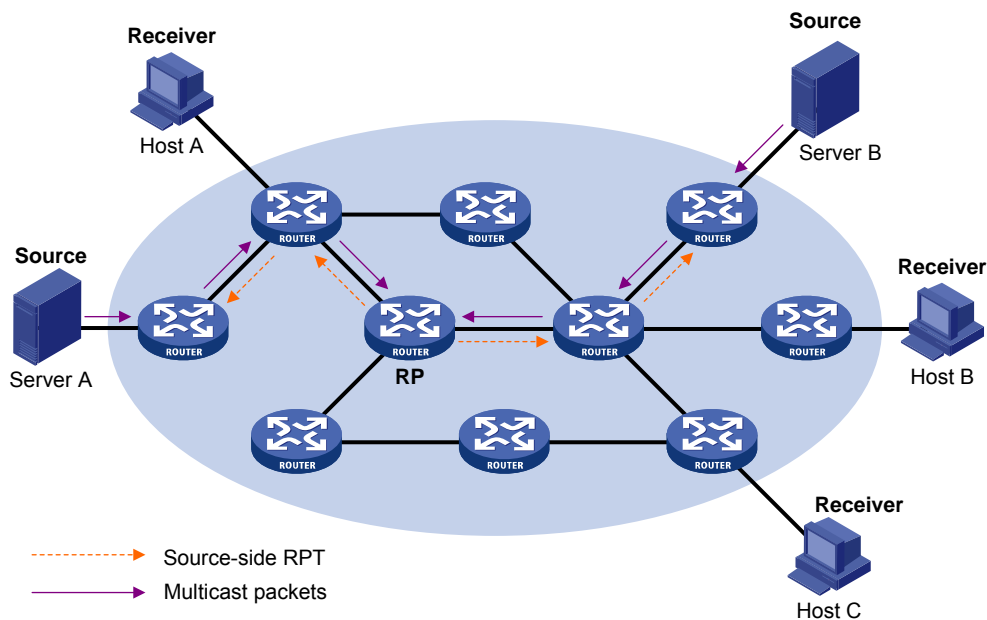


As shown in [Figure 47](#), the process for building a receiver-side RPT is similar to that for building an RPT in PIM-SM:

1. When a receiver joins multicast group G , it uses an IGMP message to inform the directly connected router.
2. After getting the receiver information, the router sends a join message, which is forwarded hop by hop to the RP of the multicast group.
3. The routers along the path from the receiver's directly connected router to the RP form an RPT branch, and each router on this branch adds a $(*, G)$ entry to its forwarding table. The $*$ means any multicast source.

When a receiver is no longer interested in the multicast data addressed to multicast group G , the directly connected router sends a prune message, which goes hop by hop along the reverse direction of the RPT to the RP. After receiving the prune message, each upstream node deletes the interface connected to the downstream node from the outgoing interface list and checks whether it has receivers in that multicast group. If not, the router continues to forward the prune message to its upstream router.

Figure 48 RPT building at the multicast source side



As shown in Figure 48, the process for building a source-side RPT is relatively simple:

1. When a multicast source sends multicast packets to multicast group G , the DF in each network segment unconditionally forwards the packets to the RP.
2. The routers along the path from the source's directly connected router to the RP form an RPT branch. Each router on this branch adds a $(*, G)$ entry to its forwarding table. The $*$ means any multicast source.

After a bidirectional RPT is built, multicast traffic is forwarded along the source-side RPT and receiver-side RPT from sources to receivers.

NOTE:

If a receiver and a multicast source are at the same side of the RP, the source-side RPT and the receiver-side RPT might meet at a node before reaching the RP. In this case, multicast packets from the multicast source to the receiver are directly forwarded by the node to the receiver, instead of by the RP.

Administrative scoping overview

Division of PIM-SM domains

Typically, a PIM-SM domain or BIDIR-PIM domain contains only one BSR, which is responsible for advertising RP-set information within the entire PIM-SM/BIDIR-PIM domain. The information for all multicast groups is forwarded within the network scope that the BSR administers. This is called the "non-scoped BSR mechanism."

To implement refined management, you can divide a PIM-SM domain or BIDIR-PIM domain into one global scope zone and multiple administratively scoped zones (admin-scope zones). This is called the "administrative scoping mechanism."

The administrative scoping mechanism effectively releases stress on the management in a single-BSR domain and enables provision of zone-specific services through private group addresses.

Admin-scope zones are divided specific to multicast groups. Zone border routers (ZBRs) form the boundary of the admin-scope zone. Each admin-scope zone maintains one BSR, which provides services for multicast groups within a specific range. Multicast protocol packets, such as assert messages and bootstrap messages, for a specific group range cannot cross the admin-scope zone boundary. Multicast group ranges to which different admin-scope zones are designated can be overlapped. A multicast group is valid only within its local admin-scope zone, and functions as a private group address.

The global scope zone maintains a BSR, which provides services for the multicast groups that do not belong to any admin-scope zone.

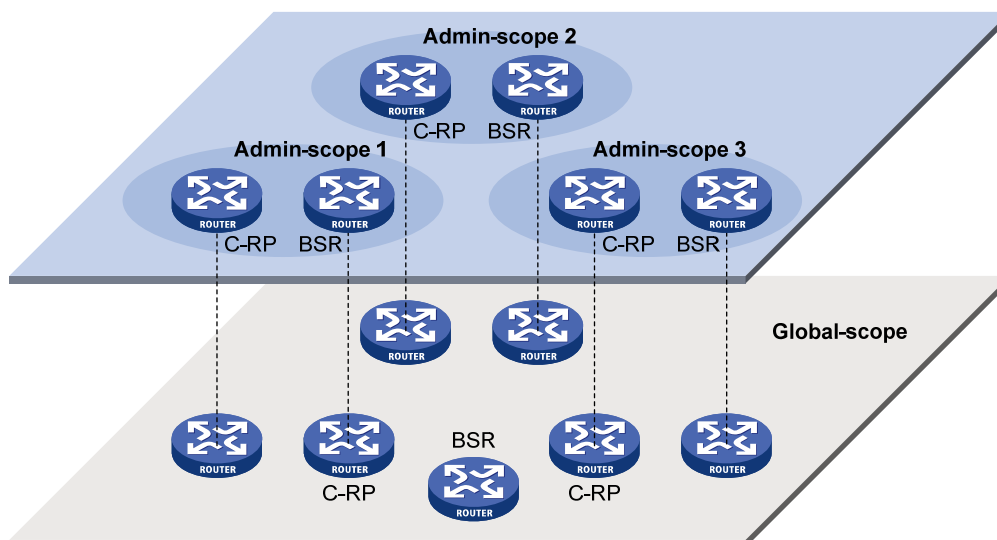
Relationship between admin-scope zones and the global scope zone

The global scope zone and each admin-scope zone have their own C-RPs and BSRs. These devices are effective only in their respective zones. That is, BSR election and RP election are implemented independently. Each admin-scope zone has its own boundary. The multicast information within a zone cannot cross this boundary in either direction. You can have a better understanding of the global-scope zone and admin-scoped zones based on geographical locations and multicast group address ranges.

- In view of geographical locations

An admin-scope zone is a logical zone for particular multicast groups. The multicast packets for such multicast groups are confined within the local admin-scope zone and cannot cross the boundary of the zone.

Figure 49 Relationship in view of geographical locations

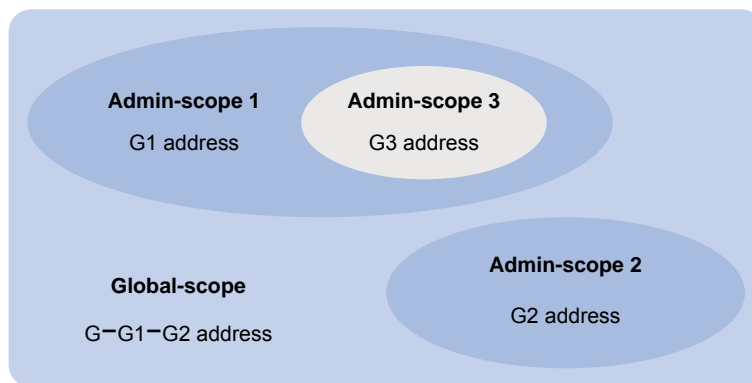


As shown in [Figure 49](#), for the multicast groups in a specific group address range, the admin-scope zones must be geographically separated and isolated. A router cannot belong to multiple admin-scope zones. In other words, different admin-scope zones contain different routers. However, the global-scope zone includes all routers in the PIM-SM domain or BIDIR-PIM domain. Multicast packets that do not belong to any admin-scope zones are forwarded in the entire PIM-SM domain or BIDIR-PIM domain.

- In view of multicast group address ranges

Each admin-scope zone provides services for specific multicast groups, of which the multicast group addresses are valid only within the local zone. The multicast groups of different admin-scoped zones might have intersections. The global-scope zone is designated to all the multicast groups other than those of the admin-scoped zones.

Figure 50 Relationship in view of multicast group address ranges



In [Figure 50](#), the admin-scoped zones 1 and 2 have no intersection, but the admin-scoped zone 3 is a subset of the admin-scoped zone 1. The global-scope zone provides services for all the multicast groups that are not covered by the admin-scoped zones 1 and 2, that is, G-G1-G2 in this case.

PIM-SSM overview

The source-specific multicast (SSM) model and the any-source multicast (ASM) model are opposites. Presently, the ASM model includes the PIM-DM and PIM-SM modes. You can implement the SSM model by leveraging part of the PIM-SM technique. It is also called "PIM-SSM."

The SSM model provides a solution for source-specific multicast. It maintains the relationships between hosts and routers through IGMPv3.

In actual application, part of IGMPv3 or PIM-SM technique is adopted to implement the SSM model. In the SSM model, receivers locate a multicast source by means of advertisements, consultancy, and so on. No RP is needed, no RPT is required, no source registration process exists, and the multicast source discovery protocol (MSDP) is not needed for discovering sources in other PIM domains.

In PIM-SSM, the term "channel" refers to a multicast group, and the term "channel subscription" refers to a join message.

The working mechanism of PIM-SSM is summarized as follows:

- Neighbor discovery
- DR election
- SPT building

Neighbor discovery

PIM-SSM uses the same neighbor discovery mechanism as in PIM-DM and PIM-SM. See "[Neighbor discovery](#)."

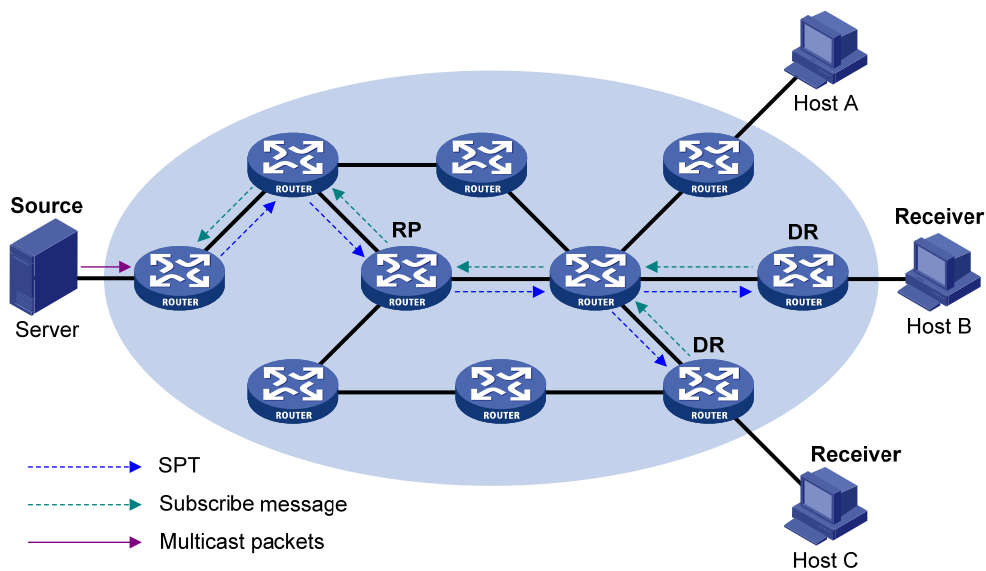
DR election

PIM-SSM uses the same DR election mechanism as in PIM-SM. See "[DR election](#)."

SPT building

The decision to build an RPT for PIM-SM or an SPT for PIM-SSM depends on whether the multicast group the receiver will join falls into the SSM group range (SSM group range reserved by IANA is 232.0.0.0/8).

Figure 51 SPT building in PIM-SSM



As shown in [Figure 51](#), Host B and Host C are multicast information receivers. They send IGMPv3 report messages to the respective DRs to express their interest in the information about the specific multicast source S.

After receiving a report message, the DR first determines whether the group address in this message falls into the SSM group range and then does the following:

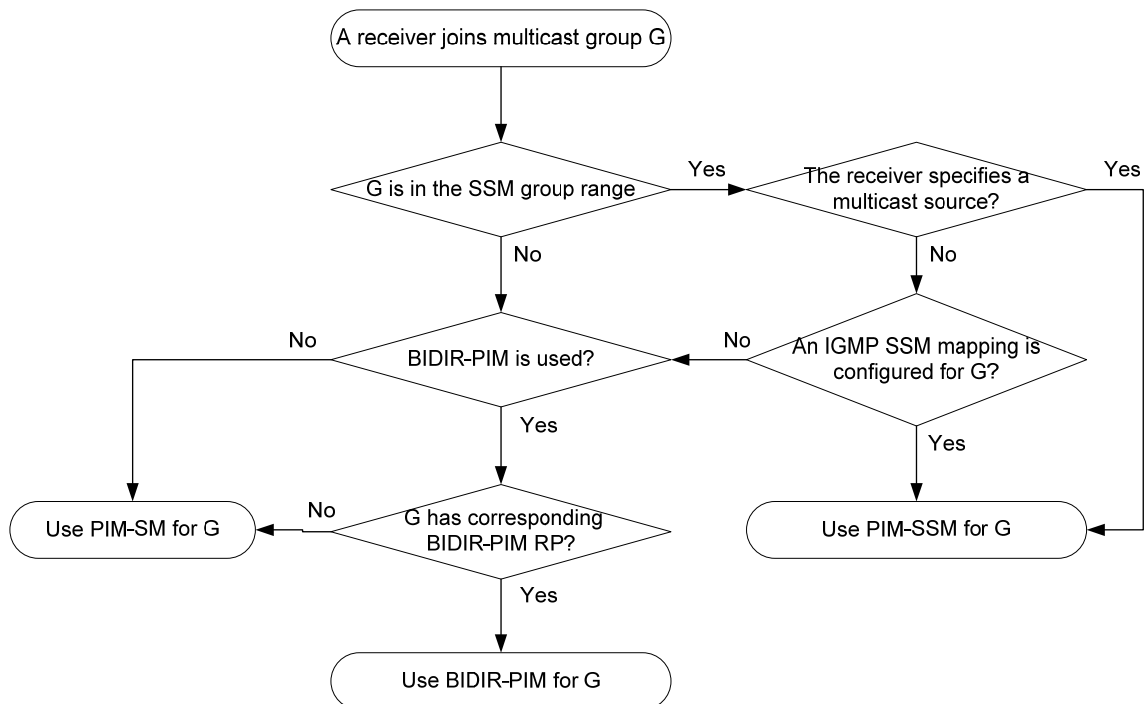
- If the group address in the message does fall into the SSM group range, the DR sends a subscribe message for channel subscription hop by hop toward the multicast source S. An (S, G) entry is created on all routers on the path from the DR to the source. An SPT is thereby built in the network, with the source S as its root and receivers as its leaves. This SPT is the transmission channel in PIM-SSM.

- If the group address in the message does not fall into the SSM group range, the receiver-side DR follows the PIM-SM process. The receiver-side DR sends a (*, G) join message to the RP, and the source-side DR registers the multicast source.

Relationships among PIM protocols

In a PIM network, PIM-DM cannot run together with PIM-SM, BIDIR-PIM, or PIM-SSM. However, PIM-SM, BIDIR-PIM, and PIM-SSM can run together. When they run together, which one is chosen for a receiver trying to join a group depends, as shown in [Figure 52](#).

Figure 52 Relationships among PIM protocols



For more information about IGMP SSM mapping, see "[Configuring IGMP \(available only on the HP 5500 EI\)](#)."

PIM support for VPNs

To support PIM for VPNs, a multicast router that runs PIM maintains an independent set of PIM neighbor table, multicast routing table, BSR information, and RP-set information for each VPN.

After receiving a multicast data packet, the multicast router checks which VPN the data packet belongs to, and then forwards the packet according to the multicast routing table for that VPN or creates a multicast routing entry for that VPN.

Protocols and standards

- RFC 3973, *Protocol Independent Multicast-Dense Mode (PIM-DM): Protocol Specification(Revised)*

- RFC 4601, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)*
- RFC 5015, *Bidirectional Protocol Independent Multicast (BIDIR-PIM)*
- RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*
- RFC 4607, *Source-Specific Multicast for IP*
- Draft-ietf-ssm-overview-05, *An Overview of Source-Specific Multicast (SSM)*

Configuring PIM-DM

PIM-DM configuration task list

Task	Remarks
Enabling PIM-DM	Required
Enabling state-refresh capability	Optional
Configuring state-refresh parameters	Optional
Configuring PIM-DM graft retry period	Optional
Configuring PIM common features	Optional

Configuration prerequisites

Before you configure PIM-DM, complete the following tasks:

- Configure any unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Determine the interval between state-refresh messages.
- Determine the minimum time to wait before receiving a new refresh message.
- Determine the TTL value of state-refresh messages.
- Determine the graft retry period.

Enabling PIM-DM

With PIM-DM enabled, a router sends hello messages periodically to discover PIM neighbors and processes messages from the PIM neighbors. When you deploy a PIM-DM domain, enable PIM-DM on all non-border interfaces of the routers.

IMPORTANT:

- All the interfaces in the same VPN instance on the same device must operate in the same PIM mode.
- PIM-DM does not work with multicast groups in the SSM group range.

Enabling PIM-DM globally on the public network

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IP multicast routing.	multicast routing-enable	Disabled by default.
3. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable PIM-DM.	pim dm	Disabled by default.

Enabling PIM-DM in a VPN instance

Step	Command	Description
1. Enter system view.	system-view	N/A
2. Create a VPN instance and enter VPN instance view.	ip vpn-instance <i>vpn-instance-name</i>	N/A
3. Configure an RD for the VPN instance.	route-distinguisher <i>route-distinguisher</i>	Not configured by default.
4. Enable IP multicast routing.	multicast routing-enable	Disabled by default.
5. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
6. Bind the interface with a VPN instance.	ip binding vpn-instance <i>vpn-instance-name</i>	By default, an interface belongs to the public network, and is not bound with any VPN instance.
7. Enable PIM-DM.	pim dm	Disabled by default.

For more information about the **ip vpn-instance**, **route-distinguisher**, and **ip binding vpn-instance** commands, see *IP Routing Command Reference*.

For more information about the **multicast routing-enable** command, see *IP Multicast Command Reference*.

Enabling state-refresh capability

Pruned interfaces resume multicast forwarding when the pruned state times out. To prevent this, the router with the multicast source attached periodically sends an (S, G) state-refresh message, which is forwarded hop by hop along the initial multicast flooding path of the PIM-DM domain, to refresh the prune timer state of all the routers on the path. A multi-access subnet can have the state-refresh capability only if the state-refresh capability is enabled on all PIM routers on the subnet.

To enable the state-refresh capability:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable the state-refresh capability.	pim state-refresh-capable	Optional Enabled by default

Configuring state-refresh parameters

The router directly connected with the multicast source periodically sends state-refresh messages. You can configure the interval for sending such messages.

A router might receive multiple state-refresh messages within a short time, and some of them might be duplicated messages. To keep a router from receiving such duplicated messages, you can configure the time that the router must wait before it receives next state-refresh message. If the router receives a new state-refresh message within the waiting time, it discards the message. If this timer times out, the router will accept a new state-refresh message, refresh its own PIM-DM state, and reset the waiting timer.

The TTL value of a state-refresh message decrements by 1 whenever it passes a router before it is forwarded to the downstream node until the TTL value comes down to 0. In a small network, a state-refresh message might cycle in the network. To effectively control the propagation scope of state-refresh messages, configure an appropriate TTL value based on the network size.

Perform the following configurations on all routers in the PIM domain.

To configure state-refresh parameters:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Configure the interval between state-refresh messages.	state-refresh-interval <i>interval</i>	Optional 60 seconds by default
4. Configure the time to wait before receiving a new state-refresh message.	state-refresh-rate-limit <i>interval</i>	Optional 30 seconds by default
5. Configure the TTL value of state-refresh messages.	state-refresh-ttl <i>tll-value</i>	Optional 255 by default

Configuring PIM-DM graft retry period

In PIM-DM, graft is the only type of message that uses the acknowledgment mechanism. In a PIM-DM domain, if a router does not receive a graft-ack message from the upstream router within the specified time after it sends a graft message, the router keeps sending new graft messages at a configurable interval (namely graft retry period), until it receives a graft-ack message from the upstream router.

To configure the graft retry period:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the graft retry period.	pim timer graft-retry <i>interval</i>	Optional 3 seconds by default

For more information about the configuration of other timers in PIM-DM, see "[Configuring PIM common timers.](#)"

Configuring PIM-SM

PIM-SM configuration task list

Task	Remarks	
Enabling PIM-SM	Required.	
Configuring an RP	Configuring a static RP	Required.
	Configuring a C-RP	Use any approach.
	Enabling auto-RP	
Configuring a BSR	Configuring C-RP timers globally	Optional.
	Configuring a C-BSR	Required.
	Configuring a PIM domain border	Optional.
	Configuring global C-BSR parameters	Optional.
	Configuring C-BSR timers	Optional.
Configuring administrative scoping	Disabling BSM semantic fragmentation	Optional.
	Enabling administrative scoping	Optional.
	Configuring an admin-scope zone boundary	Optional.
	Configuring C-BSRs for each admin-scope zone and the global-scope zone	Optional.
Configuring multicast source registration	Optional.	
Disabling the switchover to SPT	Optional.	
Configuring PIM common features	Optional.	

Configuration prerequisites

Before you configure PIM-SM, complete the following tasks:

- Configure any unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Determine the IP address of a static RP and the ACL rule defining the range of multicast groups to which the static RP is designated.
- Determine the C-RP priority and the ACL rule defining the range of multicast groups to which each C-RP is designated.
- Determine the legal C-RP address range and the ACL rule defining the range of multicast groups to which the C-RP is designated.
- Determine the C-RP-Adv interval.
- Determine the C-RP timeout.
- Determine the C-BSR priority.
- Determine the hash mask length.
- Determine the ACL rule defining a legal BSR address range.
- Determine the BS period.
- Determine the BS timeout.
- Determine the ACL rule for register message filtering.
- Determine the register suppression time.
- Determine the register probe time.
- Determine the ACL rule and sequencing rule for disabling the switchover to SPT.

Enabling PIM-SM

With PIM-SM enabled, a router sends hello messages periodically to discover PIM neighbors and processes messages from the PIM neighbors. To deploy a PIM-SM domain, enable PIM-SM on all non-border interfaces of the routers.

IMPORTANT:

All the interfaces in the same VPN instance on the same router must operate in the same PIM mode.

Enabling PIM-SM globally on the public network

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IP multicast routing.	multicast routing-enable	Disabled by default
3. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable PIM-SM.	pim sm	Disabled by default

Enabling PIM-SM in a VPN instance

Step	Command	Description
1. Enter system view.	system-view	N/A
2. Create a VPN instance and enter VPN instance view.	ip vpn-instance <i>vpn-instance-name</i>	N/A
3. Configure an RD for the VPN instance.	route-distinguisher <i>route-distinguisher</i>	Not configured by default.
4. Enable IP multicast routing.	multicast routing-enable	Disabled by default.
5. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
6. Bind the interface with a VPN instance.	ip binding vpn-instance <i>vpn-instance-name</i>	By default, an interface belongs to the public network, and is not bound with any VPN instance.
7. Enable PIM-SM.	pim sm	Disabled by default.

For more information about the **ip vpn-instance**, **route-distinguisher**, and **ip binding vpn-instance** commands, see *IP Routing Command Reference*.

For more information about the **multicast routing-enable** command, see *IP Multicast Command Reference*.

Configuring an RP

An RP can be manually configured or dynamically elected through the BSR mechanism. For a large PIM network, static RP configuration is a tedious job. Generally, static RP configuration is just a backup method for the dynamic RP election mechanism to enhance the robustness and operational manageability of a multicast network.

! IMPORTANT:

In a PIM network, if both PIM-SM and BIDIR-PIM are enabled, do not configure the same RP to provide services for PIM-SM and BIDIR-PIM simultaneously to avoid PIM routing table errors.

Configuring a static RP

If only one dynamic RP exists in a network, manually configuring a static RP can avoid communication interruption because of single-point failures. It can also avoid frequent message exchange between C-RPs and the BSR.

To enable a static RP to work normally, perform this configuration on all the routers in the PIM-SM domain and specify the same RP address.

To configure a static RP:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2.	Enter public network PIM view or VPN instance PIM view. pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3.	Configure a static RP for PIM-SM. static-rp <i>rp-address</i> [<i>acl-number</i>] [preferred]	No static RP by default

Configuring a C-RP

In a PIM-SM domain, you can configure routers that intend to become the RP as C-RPs. The BSR collects the C-RP information by receiving the C-RP-Adv messages from C-RPs or auto-RP announcements from other routers and organizes the information into an RP-set, which is flooded throughout the entire network. Then, the other routers in the network calculate the mappings between specific group ranges and the corresponding RPs based on the RP-set. HP recommends you to configure C-RPs on backbone routers.

To guard against C-RP spoofing, you must configure a legal C-RP address range and the range of multicast groups to which the C-RP is designated on the BSR. In addition, because every C-BSR can become the BSR, you must configure the same filtering policy on all C-BSRs in the PIM-SM domain.

When you configure a C-RP, ensure a relatively large bandwidth between this C-RP and the other devices in the PIM-SM domain.

To configure a C-RP:

Step	Command	Remarks
1.	Enter system view. system-view	N/A
2.	Enter public network PIM view or VPN instance PIM view. pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3.	Configure an interface to be a C-RP for PIM-SM. c-rp <i>interface-type interface-number</i> [group-policy <i>acl-number</i> priority <i>priority</i> holdtime <i>hold-interval</i> advertisement-interval <i>adv-interval</i>] *	No C-RPs are configured by default.
4.	Configure a legal C-RP address range and the range of multicast groups to which the C-RP is designated. crp-policy <i>acl-number</i>	Optional. No restrictions by default.

Enabling auto-RP

Auto-RP announcement and discovery messages are addressed to the multicast group addresses 224.0.1.39 and 224.0.1.40. With auto-RP enabled on a device, the device can receive these two types of messages and record the RP information carried in such messages.

To enable auto-RP:

Step	Command	Remarks
1.	Enter system view. system-view	N/A
2.	Enter public network PIM view or VPN instance PIM view. pim [vpn-instance <i>vpn-instance-name</i>]	N/A

Step	Command	Remarks
3. Enable auto-RP.	auto-rp enable	Disabled by default

Configuring C-RP timers globally

To enable the BSR to distribute the RP-set information within the PIM-SM domain, C-RPs must periodically send C-RP-Adv messages to the BSR. The BSR learns the RP-set information from the received messages, and encapsulates its own IP address together with the RP-set information in its bootstrap messages. The BSR then floods the bootstrap messages to all PIM routers in the network.

Each C-RP encapsulates a timeout value in its C-RP-Adv messages. After receiving a C-RP-Adv message, the BSR obtains this timeout value and starts a C-RP timeout timer. If the BSR fails to hear a subsequent C-RP-Adv message from the C-RP when this timer times out, the BSR assumes the C-RP to have expired or become unreachable.

The C-RP timers need to be configured on C-RP routers.

To configure C-RP timers globally:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance vpn-instance-name]	N/A
3. Configure the C-RP-Adv interval.	c-rp advertisement-interval interval	Optional 60 seconds by default
4. Configure C-RP timeout time.	c-rp holdtime interval	Optional 150 seconds by default

For more information about the configuration of other timers in PIM-SM, see "[Configuring PIM common timers](#)."

Configuring a BSR

A PIM-SM domain can have only one BSR, but must have at least one C-BSR. Any router can be configured as a C-BSR. Elected from C-BSRs, the BSR is responsible for collecting and advertising RP information in the PIM-SM domain.

Configuring a C-BSR

C-BSRs should be configured on routers in the backbone network. When you configure a router as a C-BSR, be sure to specify a PIM-SM-enabled interface on the router. The BSR election process is summarized as follows:

1. Initially, every C-BSR assumes itself to be the BSR of this PIM-SM domain and uses its interface IP address as the BSR address to send bootstrap messages.
2. When a C-BSR receives the bootstrap message of another C-BSR, it first compares its own priority with the other C-BSR's priority carried in the message. The C-BSR with a higher priority wins. If a

tie exists in the priority, the C-BSR with a higher IP address wins. The loser uses the winner's BSR address to replace its own BSR address and no longer assumes itself to be the BSR, and the winner retains its own BSR address and continues to assume itself to be the BSR.

BSR legal address against BSR spoofing

Configuring a legal range of BSR addresses enables filtering of bootstrap messages based on the address range, thereby preventing a maliciously configured host from masquerading as a BSR. You must make the same configuration on all routers in the PIM-SM domain. The typical BSR spoofing cases and the corresponding preventive measures are as follows:

- Some maliciously configured hosts can forge bootstrap messages to fool routers and change RP mappings. Such attacks often occur on border routers. Because a BSR is inside the network whereas hosts are outside the network, you can protect a BSR against attacks from external hosts by enabling the border routers to perform neighbor checks and RPF checks on bootstrap messages and to discard unwanted messages.
- When an attacker controls a router in the network or when an illegal router is present in the network, the attacker can configure this router as a C-BSR and make it win BSR election to control the right of advertising RP information in the network. After a router is configured as a C-BSR, it automatically floods the network with bootstrap messages. Because a bootstrap message has a TTL value of 1, the whole network will not be affected as long as the neighbor router discards these bootstrap messages. Therefore, with a legal BSR address range configured on all routers in the entire network, all these routers will discard bootstrap messages from out of the legal address range.

These preventive measures can partially protect the security of BSRs in a network. However, if an attacker controls a legal BSR, the problem will still occur.

Because a large amount of information needs to be exchanged between a BSR and the other devices in the PIM-SM domain, a relatively large bandwidth should be provided between the C-BSRs and the other devices in the PIM-SM domain.

When C-BSRs connect to other PIM routers through tunnels, static multicast routes must be configured on the PIM routers to make sure the next hop to a C-BSR is a tunnel interface. Otherwise, RPF check is affected. For more information about static multicast routes, see "[Configuring multicast routing and forwarding \(available only on the HP 5500 EI\).](#)"

To configure a C-BSR:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance vpn-instance-name]	N/A
3. Configure an interface as a C-BSR.	c-bsr interface-type interface-number [hash-length [priority]]	No C-BSRs are configured by default.
4. Configure a legal BSR address range.	bsr-policy acl-number	Optional. No restrictions on BSR address range by default.

Configuring a PIM domain border

As the administrative core of a PIM-SM domain, the BSR sends the collected RP-set information in the form of bootstrap messages to all routers in the PIM-SM domain.

A PIM domain border is a bootstrap message boundary. Each BSR has its specific service scope. A number of PIM domain border interfaces partition a network into different PIM-SM domains. Bootstrap messages cannot cross a domain border in either direction.

Perform the following configuration on routers that you want to configure as a PIM domain border.

To configure a PIM domain border:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure a PIM domain border.	pim bsr-boundary	By default, no PIM domain border is configured.

Configuring global C-BSR parameters

In each PIM-SM domain, a unique BSR is elected from C-BSRs. The C-RPs in the PIM-SM domain send advertisement messages to the BSR. The BSR summarizes the advertisement messages to form an RP-set and advertises it to all routers in the PIM-SM domain. All the routers use the same hash algorithm to get the RP address that corresponds to specific multicast groups.

You can configure the hash mask length and C-BSR priority globally, in an admin-scope zone, and in the global scope zone.

- The values configured in the global scope zone or admin-scope zone have preference over the global values.
- If you do not configure these parameters in the global scope zone or admin-scope zone, the corresponding global values will be used.

For configuration of C-BSR parameters for an admin-scope zone and global scope zone, see "[Configuring C-BSRs for each admin-scope zone and the global-scope zone.](#)"

Perform the following configuration on C-BSR routers.

To configure C-BSR parameters:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Configure the hash mask length.	c-bsr hash-length <i>hash-length</i>	Optional. 30 by default.

Step	Command	Remarks
4. Configure the C-BSR priority.	c-bsr priority <i>priority</i>	Optional. By default, the C-BSR priority is 64.

Configuring C-BSR timers

The BSR election winner multicasts its own IP address and RP-set information through bootstrap messages within the entire zone to which it is designated. The BSR floods bootstrap messages throughout the network at the interval of BS (BSR state) period. Any C-BSR that receives a bootstrap message retains the RP-set for the length of BS timeout, during which no BSR election takes place. If no bootstrap message is received from the BSR before the BS timeout timer expires, a new BSR election process is triggered among the C-BSRs.

Perform the following configuration on C-BSR routers.

To configure C-BSR timers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Configure the BS period.	c-bsr interval <i>interval</i>	Optional. By default, the BS period is determined by the formula "BS period = (BS timeout timer - 10) / 2." The default BS timeout timer is 130 seconds, so the default BS period is (130 - 10) / 2 = 60 (seconds). The BS period value must be smaller than the BS timeout timer.
4. Configure the BS timeout timer.	c-bsr holdtime <i>interval</i>	Optional. By default, the BS timeout timer is determined by the formula "BS timeout timer = BS period × 2 + 10." The default BS period is 60 seconds, so the default BS timeout timer = 60 × 2 + 10 = 130 (seconds).

NOTE:

If you configure the BS period or the BS timeout timer, the system uses the configured one instead of the default one.

Disabling BSM semantic fragmentation

Generally, a BSR periodically distributes the RP-set information in bootstrap messages within the PIM-SM domain. It encapsulates a BSM in an IP datagram and might split the datagram into fragments if the

message exceeds the maximum transmission unit (MTU). In respect of such IP fragmentation, loss of a single IP fragment leads to unavailability of the entire message.

Semantic fragmentation of BSMs can solve this issue. When a BSM exceeds the MTU, it is split to multiple bootstrap message fragments (BSMFs).

- After receiving a BSMF that contains the RP-set information of one group range, a non-BSR router updates corresponding RP-set information directly.
- If the RP-set information of one group range is carried in multiple BSMFs, a non-BSR router updates corresponding RP-set information after receiving all these BSMFs.

Because the RP-set information contained in each segment is different, loss of some IP fragments will not result in dropping of the entire message.

Generally, a BSR performs BSM semantic fragmentation according to the MTU of its BSR interface. However, the semantic fragmentation of BSMs originated because of learning of a new PIM neighbor is performed according to the MTU of the outgoing interface.

The function of BSM semantic fragmentation is enabled by default. Devices not supporting this function might deem a fragment as an entire message and learn only part of the RP-set information. Therefore, if such devices exist in the PIM-SM domain, you need to disable the semantic fragmentation function on the C-BSRs.

To disable the BSM semantic fragmentation function:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance vpn-instance-name]	N/A
3. Disable the BSM semantic fragmentation function.	undo bsm-fragment enable	By default, the BSM semantic fragmentation function is enabled.

Configuring administrative scoping

When administrative scoping is disabled, a PIM-SM domain has only one BSR. The BSR manages the whole network. To manage your network more effectively and specifically, partition the PIM-SM domain into multiple admin-scope zones. Each admin-scope zone maintains a BSR, which provides services for a specific multicast group range. The global scope zone also maintains a BSR, which provides services for all the remaining multicast groups.

Enabling administrative scoping

Before you configure an admin-scope zone, you must enable administrative scoping.

Perform the following configuration on all routers in the PIM-SM domain.

To enable administrative scoping:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Enable administrative scoping.	c-bsr admin-scope	Disabled by default

Configuring an admin-scope zone boundary

ZBRs form the boundary of each admin-scope zone. Each admin-scope zone maintains a BSR, which provides services for a specific multicast group range. Multicast protocol packets (such as assert messages and bootstrap messages) that belong to this range cannot cross the admin-scope zone boundary.

Perform the following configuration on routers that you want to configure as a ZBR.

To configure an admin-scope zone boundary:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure a multicast forwarding boundary.	multicast boundary <i>group-address</i> { <i>mask</i> <i>mask-length</i> }	By default, no multicast forwarding boundary is configured. The <i>group-address</i> { <i>mask</i> <i>mask-length</i> } argument can specify the multicast groups to which an admin-scope zone is designated, in the range of 239.0.0.0/8.

Configuring C-BSRs for each admin-scope zone and the global-scope zone

In a network with administrative scoping enabled, group-range-specific BSRs are elected from C-BSRs. C-RPs in the network send advertisement messages to the specific BSR. The BSR summarizes the advertisement messages to form an RP-set and advertises it to all routers in the specific admin-scope zone. All the routers use the same hash algorithm to get the RP address corresponding to the specific multicast group.

Configure C-BSRs for each admin-scope zone and the global-scope zone.

You can configure the hash mask length and C-BSR priority globally, in an admin-scope zone, and in the global scope zone.

- The values configured in the global scope zone or admin-scope zone have preference over the global values.
- If you do not configure these parameters in the global scope zone or admin-scope zone, the corresponding global values will be used.

For configuration of global C-BSR parameters, see "[Configuring global C-BSR parameters.](#)"

- Configure C-BSRs for each admin-scope zone

Perform the following configuration on the routers that you want to configure as C-BSRs in admin-scope zones.

To configure a C-BSR for an admin-scope zone:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance vpn-instance-name]	N/A
3. Configure a C-BSR for an admin-scope zone.	c-bsr group group-address { mask mask-length } [hash-length hash-length priority priority] *	No C-BSRs are configured for an admin-scope zone by default. The <i>group-address { mask mask-length }</i> argument can specify the multicast groups to which the C-BSR is designated, in the range of 239.0.0.0/8.

- Configure C-BSRs for the global-scope zone

Perform the following configuration on the routers that you want to configure as C-BSRs in the global-scope zone.

To configure a C-BSR for the global-scope zone:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance vpn-instance-name]	N/A
3. Configure a C-BSR for the global-scope zone.	c-bsr global [hash-length hash-length priority priority] *	No C-BSRs are configured for the global-scope zone by default.

Configuring multicast source registration

Within a PIM-SM domain, the source-side DR sends register messages to the RP, and these register messages have different multicast source or group addresses. You can configure a filtering rule to filter register messages so that the RP can provide services for specific multicast groups. If the filtering rule denies an (S, G) entry, or if the filtering rule does not define the action for this entry, the RP will send a register-stop message to the DR to stop the registration process for the multicast data.

In view of information integrity of register messages in the transmission process, you can configure the device to calculate the checksum based on the entire register messages. However, to reduce the workload of encapsulating data in register messages and for the sake of interoperability, do not use this method of checksum calculation.

When receivers stop receiving multicast data addressed to a certain multicast group through the RP (which means the RP stops serving the receivers of that multicast group), or when the RP starts receiving

multicast data from the multicast source along the SPT, the RP sends a register-stop message to the source-side DR. After receiving this message, the DR stops sending register messages encapsulated with multicast data and starts a register-stop timer. Before the register-stop timer expires, the DR sends a null register message (a register message without encapsulated multicast data) to the RP. If the DR receives a register-stop message during the register probe time, it will reset its register-stop timer. Otherwise, the DR starts sending register messages with encapsulated data again when the register-stop timer expires.

The register-stop timer is set to a random value chosen uniformly from the interval (0.5 times register_suppression_time, 1.5 times register_suppression_time) minus register_probe_time.

Configure a filtering rule for register messages on all C-RP routers and configure them to calculate the checksum based on the entire register messages. Configure the register suppression time and the register probe time on all routers that might become source-side DRs.

To configure register-related parameters:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Configure a filtering rule for register messages.	register-policy <i>acl-number</i>	Optional. No register filtering rule by default.
4. Configure the device to calculate the checksum based on the entire register messages.	register-whole-checksum	Optional. By default, the checksum is calculated based on the header of register messages.
5. Configure the register suppression time.	register-suppression-timeout <i>interval</i>	Optional. 60 seconds by default.
6. Configure the register probe time.	probe-interval <i>interval</i>	Optional 5 seconds by default.

Disabling the switchover to SPT

CAUTION:

If the switch is an RP, disabling switchover to SPT might cause multicast traffic forwarding failures on the source-side DR. When disabling switchover to SPT, be sure you fully understand its impact on your network.

If the switch acts as an RP or the receiver-side DR, it initiates a switchover to SPT process by default upon receiving the first multicast packet along the RPT. You can disable the switchover from RPT to SPT.

To disable the switchover to SPT:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Disable the switchover to SPT.	spt-switch-threshold infinity [group-policy <i>acl-number</i> [order <i>order-value</i>]]	Optional. By default, the device switches to the SPT immediately after it receives the first multicast packet.

Configuring BIDIR-PIM

BIDIR-PIM configuration task list

Task	Remarks	
Enabling PIM-SM	Required.	
Enabling BIDIR-PIM	Required.	
Configuring an RP	Configuring a static RP	Required.
	Configuring a C-RP	Use any approach.
	Enabling auto-RP	
	Configuring C-RP timers globally	Optional.
Configuring a BSR	Configuring a C-BSR	Required.
	Configuring a BIDIR-PIM domain border	Optional.
	Configuring global C-BSR parameters	Optional.
	Configuring C-BSR timers	Optional.
	Disabling BSM semantic fragmentation	Optional.
Configuring an admin-scope zone boundary	Enabling administrative scoping	Optional.
	Configuring administrative scoping	Optional.
	Configuring C-BSRs for each admin-scope zone and the global-scope zone	Optional.
Configuring PIM common features	Optional.	

Configuration prerequisites

Before you configure BIDIR-PIM, complete the following tasks:

- Configure a unicast routing protocol so that all devices in the domain can reach each other.
- Determine the IP address of a static RP and the ACL that defines the range of the multicast groups to which the static RP is designated.
- Determine the C-RP priority and the ACL that defines the range of multicast groups to which each C-RP is designated.

- Determine the legal C-RP address range and the ACL that defines the range of multicast groups to which the C-RP is designated.
- Determine the C-RP-Adv interval.
- Determine the C-RP timeout.
- Determine the C-BSR priority.
- Determine the hash mask length.
- Determine the ACL defining the legal BSR address range.
- Determine the BS period.
- Determine the BS timeout.

Enabling PIM-SM

Because BIDIR-PIM is implemented on the basis of PIM-SM, you must enable PIM-SM before enabling BIDIR-PIM. To deploy a BIDIR-PIM domain, enable PIM-SM on all non-border interfaces of the domain.

! IMPORTANT:

On a router, all interfaces in the same VPN instance must operate in the same PIM mode.

Enabling PIM-SM globally for the public network

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IP multicast routing.	multicast routing-enable	Disabled by default
3. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable PIM-SM.	pim sm	Disabled by default

Enabling PIM-SM for a VPN instance

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a VPN instance and enter VPN instance view.	ip vpn-instance <i>vpn-instance-name</i>	N/A
3. Configure an RD for the VPN instance.	route-distinguisher <i>route-distinguisher</i>	Not configured by default.
4. Enable IP multicast routing.	multicast routing-enable	Disabled by default.
5. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
6. Bind the interface with the VPN instance.	ip binding vpn-instance <i>vpn-instance-name</i>	By default, an interface belongs to the public network, and is not bound with any VPN instance.

Step	Command	Remarks
7. Enable PIM-SM.	pim sm	Disabled by default.

For more information about the **ip vpn-instance**, **route-distinguisher**, and **ip binding vpn-instance** commands, see *IP Routing Command Reference*.

Enabling BIDIR-PIM

Perform this configuration on all routers in the BIDIR-PIM domain.

To enable BIDIR-PIM:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance vpn-instance-name]	N/A
3. Enable BIDIR-PIM.	bidir-pim enable	Disabled by default

Configuring an RP

An RP can be manually configured or dynamically elected through the BSR mechanism. For a large PIM network, static RP configuration is a tedious job. Generally, static RP configuration is just used as a backup means for the dynamic RP election mechanism to enhance the robustness and operation manageability of a multicast network.

When both PIM-SM and BIDIR-PIM run on the PIM network, do not use the same RP to provide services for PIM-SM and BIDIR-PIM. Otherwise, exceptions might occur to the PIM routing table.

Configuring a static RP

If only one dynamic RP exists in a network, manually configuring a static RP can avoid communication interruption because of single-point failures and avoid frequent message exchange between C-RPs and the BSR.

In BIDIR-PIM, a static RP can be specified with a virtual IP address. For example, if the IP addresses of the interfaces at the two ends of a link are 10.1.1.1/24 and 10.1.1.2/24, you can specify a virtual IP address, like 10.1.1.100/24, for the static RP. As a result, the link becomes an RPL.

To make a static RP to work normally, you must perform this configuration on all routers in the BIDIR-PIM domain and specify the same RP address.

To configure a static RP:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2.	Enter public network PIM view or VPN instance PIM view. pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3.	Configure a static RP for BIDIR-PIM. static-rp <i>rp-address</i> [<i>acl-number</i>] [preferred] bidir	No static RP by default

Configuring a C-RP

In a BIDIR-PIM domain, you can configure routers that intend to become the RP as C-RPs. The BSR collects the C-RP information by receiving the C-RP-Adv messages from C-RPs or auto-RP announcements from other routers and organizes the information into an RP-set, which is flooded throughout the entire network. Then, the other routers in the network calculate the mappings between specific group ranges and the corresponding RPs based on the RP-set. HP recommends that you configure C-RPs on backbone routers.

To guard against C-RP spoofing, configure a legal C-RP address range and the range of multicast groups to which the C-RP is designated on the BSR. In addition, because every C-BSR has a chance to become the BSR, you must configure the same filtering policy on all C-BSRs in the BIDIR-PIM domain.

When you configure a C-RP, ensure a relatively large bandwidth between this C-RP and the other devices in the BIDIR-PIM domain.

To configure a C-RP:

Step	Command	Remarks
1.	Enter system view. system-view	N/A
2.	Enter public network PIM view or VPN instance PIM view. pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3.	Configure an interface to be a C-RP for BIDIR-PIM. c-rp <i>interface-type interface-number</i> [group-policy <i>acl-number</i> priority <i>priority</i> holdtime <i>hold-interval</i> advertisement-interval <i>adv-interval</i>] * bidir	No C-RP is configured by default.

Enabling auto-RP

Auto-RP announcement and discovery messages are addressed to the multicast group addresses 224.0.1.39 and 224.0.1.40. With auto-RP enabled on a device, the device can receive these two types of messages and record the RP information carried in such messages.

To enable auto-RP:

Step	Command	Remarks
1.	Enter system view. system-view	N/A
2.	Enter public network PIM view or VPN instance PIM view. pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3.	Enable auto-RP. auto-rp enable	Disabled by default

Configuring C-RP timers globally

To enable the BSR to distribute the RP-set information within the BIDIR-PIM domain, C-RPs must periodically send C-RP-Adv messages to the BSR. The BSR learns the RP-set information from the received messages, and encapsulates its own IP address together with the RP-set information in its bootstrap messages. The BSR then floods the bootstrap messages to all PIM routers in the network.

Each C-RP encapsulates a timeout value in its C-RP-Adv messages. After receiving a C-RP-Adv message, the BSR obtains this timeout value and starts a C-RP timeout timer. If the BSR fails to hear a subsequent C-RP-Adv message from the C-RP within the timeout interval, the BSR assumes the C-RP to have expired or become unreachable.

The C-RP timers need to be configured on C-RP routers.

To configure C-RP timers globally:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance vpn-instance-name]	N/A
3. Configure the C-RP-Adv interval.	c-rp advertisement-interval interval	Optional 60 seconds by default
4. Configure C-RP timeout time.	c-rp holdtime interval	Optional 150 seconds by default

For more information about the configuration of other timers in BIDIR-PIM, see "[Configuring PIM common timers.](#)"

Configuring a BSR

A BIDIR-PIM domain can have only one BSR, but must have at least one C-BSR. Any router can be configured as a C-BSR. Elected from C-BSRs, the BSR collects and advertises RP information in the BIDIR-PIM domain.

Configuring a C-BSR

C-BSRs must be configured on routers in the backbone network. When you configure a router as a C-BSR, be sure to specify a PIM-SM-enabled interface on the router. The BSR election process is as follows:

1. Initially, every C-BSR assumes itself to be the BSR of the BIDIR-PIM domain, and uses its interface IP address as the BSR address to send bootstrap messages.
2. When a C-BSR receives the bootstrap message of another C-BSR, it first compares its own priority with the other C-BSR's priority carried in message. The C-BSR with a higher priority wins. If a tie exists in the priority, the C-BSR with a higher IP address wins. The loser uses the winner's BSR address to replace its own BSR address and no longer assumes itself to be the BSR, and the winner retains its own BSR address and continues assuming itself to be the BSR.

Configuring a legal range of BSR addresses enables filtering of bootstrap messages based on the address range, thus to prevent a maliciously configured host from masquerading as a BSR. The same configuration must be made on all routers in the BIDIR-PIM domain. The following are typical BSR spoofing cases and the corresponding preventive measures:

- Some maliciously configured hosts can forge bootstrap messages to fool routers and change RP mappings. Such attacks often occur on border routers. Because a BSR is inside the network whereas hosts are outside the network, you can protect a BSR against attacks from external hosts by enabling the border routers to perform neighbor checks and RPF checks on bootstrap messages and discard unwanted messages.
- When a router in the network is controlled by an attacker or when an illegal router is present in the network, the attacker can configure this router as a C-BSR and make it win BSR election to control the right of advertising RP information in the network. After being configured as a C-BSR, a router automatically floods the network with bootstrap messages. Because a bootstrap message has a TTL value of 1, the whole network will not be affected as long as the neighbor router discards these bootstrap messages. Therefore, with a legal BSR address range configured on all routers in the entire network, all these routers will discard bootstrap messages from out of the legal address range.

The preventive measures can partially protect the security of BSRs in a network. If a legal BSR is controlled by an attacker, the preceding problem will still occur.

Because a large amount of information needs to be exchanged between a BSR and the other devices in the BIDIR-PIM domain, a relatively large bandwidth should be provided between the C-BSRs and the other devices in the BIDIR-PIM domain.

When C-BSRs connect to other PIM routers through tunnels, static multicast routes must be configured on the PIM routers to make sure the next hop to a C-BSR is a tunnel interface. Otherwise, RPF check is affected. For more information about static multicast routes, see "[Configuring multicast routing and forwarding \(available only on the HP 5500 EI\)](#)."

To configure a C-BSR:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance vpn-instance-name]	N/A
3. Configure an interface as a C-BSR.	c-bsr interface-type interface-number [hash-length [priority]]	No C-BSRs are configured by default.
4. Configure a legal BSR address range.	bsr-policy acl-number	Optional. No restrictions on BSR address range by default.

Configuring a BIDIR-PIM domain border

As the administrative core of a BIDIR-PIM domain, the BSR sends the collected RP-Set information in the form of bootstrap messages to all routers in the BIDIR-PIM domain.

A BIDIR-PIM domain border is a bootstrap message boundary. Each BSR has its specific service scope. A number of BIDIR-PIM domain border interfaces partition a network into different BIDIR-PIM domains. Bootstrap messages cannot cross a domain border in either direction.

Perform the following configuration on routers that you want to configure as the PIM domain border.

To configure a BIDIR-PIM domain border:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure a BIDIR-PIM domain border.	pim bsr-boundary	By default, no BIDIR-PIM domain border is configured.

Configuring global C-BSR parameters

In each BIDIR-PIM domain, a unique BSR is elected from C-BSRs. The C-RPs in the BIDIR-PIM domain send advertisement messages to the BSR. The BSR summarizes the advertisement messages to form an RP-set and advertises it to all routers in the BIDIR-PIM domain. All the routers use the same hash algorithm to get the RP address corresponding to specific multicast groups.

The following rules apply to the hash mask length and C-BSR priority:

- You can configure the hash mask length and C-BSR priority globally, in an admin-scope zone, and in the global scope zone.
- The values configured in the global scope zone or admin-scope zone have preference over the global values.
- If you do not configure these parameters in the global scope zone or admin-scope zone, the corresponding global values will be used.

For configuration of C-BSR parameters for an admin-scope zone and global scope zone, see "[Configuring C-BSRs for each admin-scope zone and the global-scope zone.](#)"

Perform the following configuration on C-BSR routers.

To configure global C-BSR parameters:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Configure the hash mask length.	c-bsr hash-length <i>hash-length</i>	Optional. 30 by default.

Step	Command	Remarks
4. Configure the C-BSR priority.	c-bsr priority <i>priority</i>	Optional. 64 by default.

Configuring C-BSR timers

The BSR election winner multicasts its own IP address and RP-Set information through bootstrap messages within the entire zone to which it is designated. The BSR floods bootstrap messages throughout the network at the interval of BS (BSR state) period. Any C-BSR that receives a bootstrap message retains the RP-set for the length of BS timeout, during which no BSR election takes place. If no bootstrap message is received from the BSR before the BS timeout timer expires, a new BSR election process is triggered among the C-BSRs.

Perform the following configuration on C-BSR routers.

To configure C-BSR timers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance vpn-instance-name]	N/A
3. Configure the BS period.	c-bsr interval <i>interval</i>	Optional. By default, the BS period is determined by the formula "BS period = (BS timeout timer – 10) / 2." The default BS timeout timer is 130 seconds, so the default BS period is (130 – 10) / 2 = 60 (seconds). The BS period value must be smaller than the BS timeout timer.
4. Configure the BS timeout timer.	c-bsr holdtime <i>interval</i>	Optional. By default, the BS timeout timer is determined by the formula "BS timeout timer = BS period × 2 + 10." The default BS period is 60 seconds, so the default BS timeout timer is 60 × 2 + 10 = 130 (seconds).

NOTE:

If you configure the BS period or the BS timeout timer, the system uses the configured one instead of the default one.

Disabling BSM semantic fragmentation

Generally, a BSR periodically distributes the RP-set information in bootstrap messages within the BIDIR-PIM domain. It encapsulates a BSM in an IP datagram and might split the datagram into fragments

if the message exceeds the MTU. In respect of such IP fragmentation, loss of a single IP fragment leads to unavailability of the entire message.

Semantic fragmentation of BSMs can solve this issue. When a BSM exceeds the MTU, it is split to multiple bootstrap message fragments (BSMFs).

- After receiving a BSMF that contains the RP-set information of one group range, a non-BSR router updates corresponding RP-set information directly.
- If the RP-set information of one group range is carried in multiple BSMFs, a non-BSR router updates corresponding RP-set information after receiving all these BSMFs.

Because the RP-set information contained in each segment is different, loss of some IP fragments will not result in dropping of the entire message.

Generally, a BSR performs BSM semantic fragmentation according to the MTU of its BSR interface. However, the semantic fragmentation of BSMs originated due to learning of a new PIM neighbor is performed according to the MTU of the outgoing interface.

The function of BSM semantic fragmentation is enabled by default. Devices not supporting this function might deem a fragment as an entire message, thus learning only part of the RP-set information. Therefore, if such devices exist in the BIDIR-PIM domain, you need to disable the semantic fragmentation function on the C-BSRs.

To disable the BSM semantic fragmentation function:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance vpn-instance-name]	N/A
3. Disable the BSM semantic fragmentation function.	undo bsm-fragment enable	By default, the BSM semantic fragmentation function is enabled.

Configuring administrative scoping

With administrative scoping disabled, a BIDIR-PIM domain has only one BSR. The BSR manages the whole network. To manage your network more effectively and specifically, partition the BIDIR-PIM domain into multiple admin-scope zones. Each admin-scope zone maintains a BSR, which provides services for a specific multicast group range. The global scope zone also maintains a BSR, which provides services for all the rest multicast groups.

Enabling administrative scoping

Before you configure an admin-scope zone, you must enable administrative scoping first.

Perform the following configuration on all routers in the BIDIR-PIM domain.

To enable administrative scoping:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Enable administrative scoping.	c-bsr admin-scope	Disabled by default

Configuring an admin-scope zone boundary

The boundary of each admin-scope zone is formed by ZBRs. Each admin-scope zone maintains a BSR, which provides services for a specific multicast group range. Multicast protocol packets (such as assert messages and bootstrap messages) that belong to this range cannot cross the admin-scope zone boundary.

Perform the following configuration on routers that you want to configure as a ZBR.

To configure an admin-scope zone boundary:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure a multicast forwarding boundary.	multicast boundary <i>group-address</i> { <i>mask</i> <i>mask-length</i> }	By default, no multicast forwarding boundary is configured. The <i>group-address</i> { <i>mask</i> <i>mask-length</i> } argument can specify the multicast groups to which the admin-scope zone is designated, in the range of 239.0.0.0/8.

Configuring C-BSRs for each admin-scope zone and the global-scope zone

In a network with administrative scoping enabled, group-range-specific BSRs are elected from C-BSRs. C-RPs in the network send advertisement messages to the specific BSR. The BSR summarizes the advertisement messages to form an RP-set and advertises it to all routers in the specific admin-scope zone. All the routers use the same hash algorithm to get the RP address corresponding to the specific multicast group.

Configure C-BSRs for each admin-scope zone and the global-scope zone.

You can configure the hash mask length and C-BSR priority globally, in an admin-scope zone, and in the global scope zone.

- The values configured in the global scope zone or admin-scope zone have preference over the global values.
- If you do not configure these parameters in the global scope zone or admin-scope zone, the corresponding global values will be used.

For configuration of global C-BSR parameters, see "[Configuring global C-BSR parameters.](#)"

- Configure C-BSRs for each admin-scope zone

Perform the following configuration on the routers that you want to configure as C-BSRs in admin-scope zones.

To configure a C-BSR for an admin-scope zone:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Configure a C-BSR for an admin-scope zone.	c-bsr group <i>group-address</i> { <i>mask</i> <i>mask-length</i> } [hash-length <i>hash-length</i> priority <i>priority</i>] *	No C-BSRs are configured for an admin-scope zone by default. The <i>group-address</i> { <i>mask</i> <i>mask-length</i> } argument can specify the multicast groups to which the C-BSR is designated, in the range of 239.0.0.0/8.

- Configure C-BSRs for the global-scope zone

Perform the following configuration on the routers that you want to configure as C-BSRs in the global-scope zone.

To configure a C-BSR for the global-scope zone:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Configure a C-BSR for the global-scope zone.	c-bsr global [hash-length <i>hash-length</i> priority <i>priority</i>] *	No C-BSRs are configured for the global-scope zone by default.

Configuring PIM-SSM

PIM-SSM needs the support of IGMPv3. Be sure to enable IGMPv3 on PIM routers with multicast receivers.

PIM-SSM configuration task list

Task	Remarks
Enabling PIM-SSM	Required
Configuring the SSM group range	Optional
Configuring PIM common features	Optional

Configuration prerequisites

Before you configure PIM-SSM, complete the following tasks:

- Configure any unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Determine the SSM group range.

Enabling PIM-SM

The implementation of the SSM model is based on some subsets of PIM-SM. Therefore, you must enable PIM-SM before configuring PIM-SSM.

When deploying a PIM-SSM domain, enable PIM-SM on non-border interfaces of the routers.



IMPORTANT:

All the interfaces in the same VPN instance on the same device must operate in the same PIM mode.

Enabling PIM-SM globally on the public network

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IP multicast routing.	multicast routing-enable	Disabled by default
3. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable PIM-SM.	pim sm	Disabled by default

Enabling PIM-SM in a VPN instance

Step	Command	Description
1. Enter system view.	system-view	N/A
2. Create a VPN instance and enter VPN instance view.	ip vpn-instance <i>vpn-instance-name</i>	N/A
3. Configure an RD for the VPN instance.	route-distinguisher <i>route-distinguisher</i>	No RD is configured by default.
4. Enable IP multicast routing.	multicast routing-enable	Disabled by default.
5. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
6. Bind the interface with a VPN instance.	ip binding vpn-instance <i>vpn-instance-name</i>	By default, an interface belongs to the public network, and it is not bound with any VPN instance.
7. Enable PIM-SM.	pim sm	Disabled by default.

For more information about the **ip vpn-instance**, **route-distinguisher**, and **ip binding vpn-instance** commands, see *IP Routing Command Reference*.

Configuring the SSM group range

As for whether the information from a multicast source is delivered to the receivers based on the PIM-SSM model or the PIM-SM model, this depends on whether the group address in the (S, G) channel subscribed by the receivers falls into the SSM group range. All PIM-SM-enabled interfaces assume that multicast groups within this address range are using the PIM-SSM model.

Configuration guidelines

- Make sure that the same SSM group range is configured on all routers in the entire domain. Otherwise, multicast information cannot be delivered through the SSM model.
- When a member of a multicast group in the SSM group range sends an IGMPv1 or IGMPv2 report message, the device does not trigger a (*, G) join.

Configuration procedure

Perform the following configuration on all routers in the PIM-SSM domain.

To configure an SSM multicast group range:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance vpn-instance-name]	N/A
3. Configure the SSM group range.	ssm-policy acl-number	Optional 232.0.0.0/8 by default

Configuring PIM common features

For the functions or parameters that can be configured in both PIM view and interface view described in this section:

- In PIM view, the configuration is effective on all interfaces. In interface view, the configuration is effective on only the current interface.
- If the same function or parameter is configured in both PIM view and interface view, the configuration in interface view has preference over the configuration in PIM view, regardless of the configuration sequence.

PIM common feature configuration task list

Task	Remarks
Configuring a multicast data filter	Optional

Task	Remarks
Configuring a hello message filter	Optional
Configuring PIM hello options	Optional
Configuring the prune delay	Optional
Configuring PIM common timers	Optional
Configuring join/prune message sizes	Optional
Configuring PIM to work with BFD	Optional
Setting the DSCP value for PIM messages	Optional

Configuration prerequisites

Before you configure PIM common features, complete the following tasks:

- Configure any unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Configure PIM-DM, or PIM-SM, or PIM-SSM.
- Determine the ACL rule for filtering multicast data.
- Determine the ACL rule defining a legal source address range for hello messages.
- Determine the priority for DR election (global value/interface level value).
- Determine the PIM neighbor timeout time (global value/interface value).
- Determine the prune message delay (global value/interface level value).
- Determine the prune override interval (global value/interface level value).
- Determine the prune delay.
- Determine the hello interval (global value/interface level value).
- Determine the maximum delay between hello message (interface level value).
- Determine the assert timeout time (global value/interface value).
- Determine the join/prune interval (global value/interface level value).
- Determine the join/prune timeout (global value/interface value).
- Determine the multicast source lifetime.
- Determine the maximum size of join/prune messages.
- Determine the maximum number of (S, G) entries in a join/prune message.
- Determine the DSCP value for PIM messages.

Configuring a multicast data filter

In either a PIM-DM domain or a PIM-SM domain, routers can check passing-by multicast data based on the configured filtering rules and determine whether to continue forwarding the multicast data. In other

words, PIM routers can act as multicast data filters. These filters can help implement traffic control on one hand, and control the information available to receivers downstream to enhance data security on the other hand.

Generally, a smaller distance from the filter to the multicast source results in a more remarkable filtering effect.

This filter works not only on independent multicast data but also on multicast data encapsulated in register messages.

To configure a multicast data filter:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Configure a multicast group filter.	source-policy <i>acl-number</i>	No multicast data filter by default

Configuring a hello message filter

Along with the wide applications of PIM, the security requirement for the protocol is becoming increasingly demanding. The establishment of correct PIM neighboring relationships is the prerequisite for secure application of PIM. You can configure a legal source address range for hello messages on interfaces of routers to ensure the correct PIM neighboring relationships, guarding against PIM message attacks.

To configure a hello message filter:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure a hello message filter.	pim neighbor-policy <i>acl-number</i>	No hello message filter is configured by default.

NOTE:

With the hello message filter configured, if hello messages of an existing PIM neighbor fail to pass the filter, the PIM neighbor will be removed automatically when it times out.

Configuring PIM hello options

In either a PIM-DM domain or a PIM-SM domain, the hello messages sent among routers contain the following configurable options:

- **DR_Priority** (for PIM-SM only)—Priority for DR election. The device with the highest priority wins the DR election. You can configure this parameter on all the routers in a multi-access network directly connected to multicast sources or receivers.
- **Holdtime**—The timeout time of PIM neighbor reachability state. When this timer times out, if the router has received no hello message from a neighbor, it assumes that this neighbor has expired or become unreachable.
- **LAN_Prune_Delay**—The delay of prune messages on a multi-access network. This option consists of LAN-delay (prune message delay), override-interval, and neighbor tracking flag. If the LAN-delay or override-interval values of different PIM routers on a multi-access subnet are different, the largest value takes effect. If you want to enable neighbor tracking, be sure to enable the neighbor tracking feature on all PIM routers on a multi-access subnet.

The LAN-delay setting will cause the upstream routers to delay processing received prune messages. The override-interval sets the length of time that a downstream router can wait before sending a prune override message. When a router receives a prune message from a downstream router, it does not perform the prune action immediately. Instead, it maintains the current forwarding state for a period of LAN-delay plus override-interval. If the downstream router needs to continue receiving multicast data, it must send a join message within the prune override interval. Otherwise, the upstream router will perform the prune action when the period of LAN-delay plus override-interval times out.

A hello message sent from a PIM router contains a generation ID option. The generation ID is a random value for the interface on which the hello message is sent. Normally, the generation ID of a PIM router does not change unless the status of the router changes (for example, when PIM is just enabled on the interface or the device is restarted). When the router starts or restarts sending hello messages, it generates a new generation ID. If a PIM router finds that the generation ID in a hello message from the upstream router has changed, it assumes that the status of the upstream neighbor is lost or that the upstream neighbor has changed. In this case, it triggers a join message for state update.

If you disable join suppression (namely, enable neighbor tracking), be sure to disable the join suppression feature on all PIM routers on a multi-access subnet. Otherwise, the upstream router will fail to explicitly track join messages from downstream routers.

Configuring hello options globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance vpn-instance-name]	N/A
3. Configure the priority for DR election.	hello-option dr-priority priority	Optional. 1 by default.
4. Configure PIM neighbor timeout time.	hello-option holdtime interval	Optional. 105 seconds by default.
5. Configure the prune message delay time (LAN-delay).	hello-option lan-delay interval	Optional. 500 milliseconds by default.

Step	Command	Remarks
6. Configure the prune override interval.	hello-option override-interval <i>interval</i>	Optional. 2500 milliseconds by default.
7. Disable join suppression.	hello-option neighbor-tracking	Enabled by default.

Configuring hello options on an interface

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the priority for DR election.	pim hello-option dr-priority <i>priority</i>	Optional. 1 by default.
4. Configure PIM neighbor timeout time.	pim hello-option holdtime <i>interval</i>	Optional. 105 seconds by default.
5. Configure the prune message delay time (LAN-delay).	pim hello-option lan-delay <i>interval</i>	Optional. 500 milliseconds by default.
6. Configure the prune override interval.	pim hello-option override-interval <i>interval</i>	Optional. 2,00 milliseconds by default.
7. Disable join suppression.	pim hello-option neighbor-tracking	Enabled by default.
8. Configure the interface to reject hello messages without a generation ID.	pim require-genid	By default, hello messages without Generation_ID are accepted.

Configuring the prune delay

Configuring a prune delay interval on an upstream router on a shared network segment can make the upstream router not perform the prune action immediately after it receives the prune message from its downstream router. Instead, the upstream router maintains the current forwarding state for a period of time that the prune delay interval defines. In this period, if the upstream router receives a join message from the downstream router, it cancels the prune action. Otherwise, it performs the prune action.

To configure the prune delay time:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Configure the prune delay interval.	prune delay <i>interval</i>	Optional. By default, the prune delay is not configured.

Configuring PIM common timers

PIM routers discover PIM neighbors and maintain PIM neighboring relationships with other routers by periodically sending out hello messages.

After receiving a hello message, a PIM router waits a random period, which is smaller than the maximum delay between hello messages, before sending a hello message. This delay avoids collisions that occur when multiple PIM routers send hello messages simultaneously.

A PIM router periodically sends join/prune messages to its upstream for state update. A join/prune message contains the join/prune timeout time. The upstream router sets a join/prune timeout timer for each pruned downstream interface.

Any router that has lost assert election will prune its downstream interface and maintain the assert state for a period of time. When the assert state times out, the assert losers will resume multicast forwarding.

When a router fails to receive subsequent multicast data from multicast source *S*, the router does not immediately delete the corresponding (*S*, *G*) entry. Instead, it maintains the (*S*, *G*) entry for a period of time (namely, the multicast source lifetime) before deleting the (*S*, *G*) entry.

NOTE:

If no special networking requirements are raised, use the default settings.

Configuring PIM common timers globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance vpn-instance-name]	N/A
3. Configure the hello interval.	timer hello interval	Optional. 30 seconds by default.
4. Configure the join/prune interval.	timer join-prune interval	Optional. 60 seconds by default.
5. Configure the join/prune timeout time.	holdtime join-prune interval	Optional. 210 seconds by default.
6. Configure assert timeout time.	holdtime assert interval	Optional. 180 seconds by default.
7. Configure the multicast source lifetime.	source-lifetime interval	Optional. 210 seconds by default.

Configuring PIM common timers on an interface

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the hello interval.	pim timer hello <i>interval</i>	Optional. 30 seconds by default.
4. Configure the maximum delay between hello messages.	pim triggered-hello-delay <i>interval</i>	Optional. 5 seconds by default.
5. Configure the join/prune interval.	pim timer join-prune <i>interval</i>	Optional. 60 seconds by default.
6. Configure the join/prune timeout time.	pim holdtime join-prune <i>interval</i>	Optional. 210 seconds by default.
7. Configure assert timeout time.	pim holdtime assert <i>interval</i>	Optional. 180 seconds by default.

Configuring join/prune message sizes

A large size of a join/prune message might result in loss of a larger amount of information if a message is lost. You can set a small value for the size of each join/prune message to reduce the impact in case of the loss of a message.

By controlling the maximum number of (S, G) entries in a join/prune message, you can effectively reduce the number of (S, G) entries sent per unit of time.

! IMPORTANT:

If PIM snooping-enabled switches are deployed in the PIM network, be sure to set a value no greater than the path MTU for the maximum size of each join/prune message on the receiver-side edge PIM devices

To configure join/prune message sizes:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network PIM view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Configure the maximum size of each join/prune message.	jp-pkt-size <i>packet-size</i>	Optional. 8100 bytes by default.
4. Configure the maximum number of (S, G) entries in a join/prune message.	jp-queue-size <i>queue-size</i>	Optional. 1020 by default.

Configuring PIM to work with BFD

PIM uses hello messages to elect a DR for a multi-access network. The elected DR will be the only multicast forwarder on the multi-access network.

If the DR fails, a new DR election process will start after the DR is aged out. However, it might take a long period of time. To start a new DR election process immediately after the original DR fails, enable PIM to work with Bidirectional Forwarding Detection (BFD) on a multi-access network to detect failures of the links among PIM neighbors. You must enable PIM to work with BFD on all PIM-capable routers on a multi-access network, so that the PIM neighbors can fast detect DR failures and start a new DR election process.

For more information about BFD, see *High Availability Configuration Guide*.

Before you configure this feature on an interface, be sure to enable PIM-DM or PIM-SM on the interface.

To enable PIM to work with BFD:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type interface-number</i>	N/A
3. Enable PIM to work with BFD.	pim bfd enable	Disabled by default

Setting the DSCP value for PIM messages

IPv4 uses an eight-bit ToS field to identify type of service for IP packets. As defined in RFC 2474, the first six bits contains the DSCP priority for prioritizing traffic in the network and the last two bits are reserved.

To set the DSCP value for PIM messages:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network IGMP view or VPN instance PIM view.	pim [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Set the DSCP value for PIM messages	dscp <i>dscp-value</i>	Optional. By default, the DSCP value in PIM messages is 48.

Displaying and maintaining PIM

Task	Command	Remarks
Display the BSR information in the PIM-SM domain and locally configured C-RP information in effect.	display pim [all-instance vpn-instance <i>vpn-instance-name</i>] bsr-info [{ begin exclude include } <i>regular-expression</i>]	Available in any view

Task	Command	Remarks
Display the information of unicast routes used by PIM.	display pim [all-instance vpn-instance <i>vpn-instance-name</i>] claimed-route [<i>source-address</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the number of PIM control messages.	display pim [all-instance vpn-instance <i>vpn-instance-name</i>] control-message counters [message-type { probe register register-stop }] [interface <i>interface-type interface-number</i> message-type { assert bsr crp graft graft-ack hello join-prune state-refresh }] *] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the DF information of BIDIR-PIM.	display pim [all-instance vpn-instance <i>vpn-instance-name</i>] df-info [<i>rp-address</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the information about unacknowledged PIM-DM graft messages.	display pim [all-instance vpn-instance <i>vpn-instance-name</i>] grafts [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the PIM information on an interface or all interfaces.	display pim [all-instance vpn-instance <i>vpn-instance-name</i>] interface [<i>interface-type interface-number</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the information of join/prune messages to send.	display pim [all-instance vpn-instance <i>vpn-instance-name</i>] join-prune mode { sm [flags <i>flag-value</i>] ssm } [interface <i>interface-type interface-number</i> neighbor <i>neighbor-address</i>] * [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display PIM neighboring information.	display pim [all-instance vpn-instance <i>vpn-instance-name</i>] neighbor [interface <i>interface-type interface-number</i> <i>neighbor-address</i> verbose] * [{ begin exclude include } <i>regular-expression</i>]	Available in any view

Task	Command	Remarks
Display the content of the PIM routing table.	display pim [all-instance vpn-instance <i>vpn-instance-name</i>] routing-table [<i>group-address</i> [mask { <i>mask-length</i> <i>mask</i> }] <i>source-address</i> [mask { <i>mask-length</i> <i>mask</i> }] incoming-interface [<i>interface-type</i> <i>interface-number</i> register] outgoing-interface { include exclude match } { <i>interface-type</i> <i>interface-number</i> register } mode <i>mode-type</i> flags <i>flag-value</i> fsm] * [[{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the RP information.	display pim [all-instance vpn-instance <i>vpn-instance-name</i>] rp-info [<i>group-address</i>] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view
Reset PIM control message counters.	reset pim [all-instance vpn-instance <i>vpn-instance-name</i>] control-message counters [interface <i>interface-type</i> <i>interface-number</i>]	Available in user view

PIM configuration examples

PIM-DM configuration example

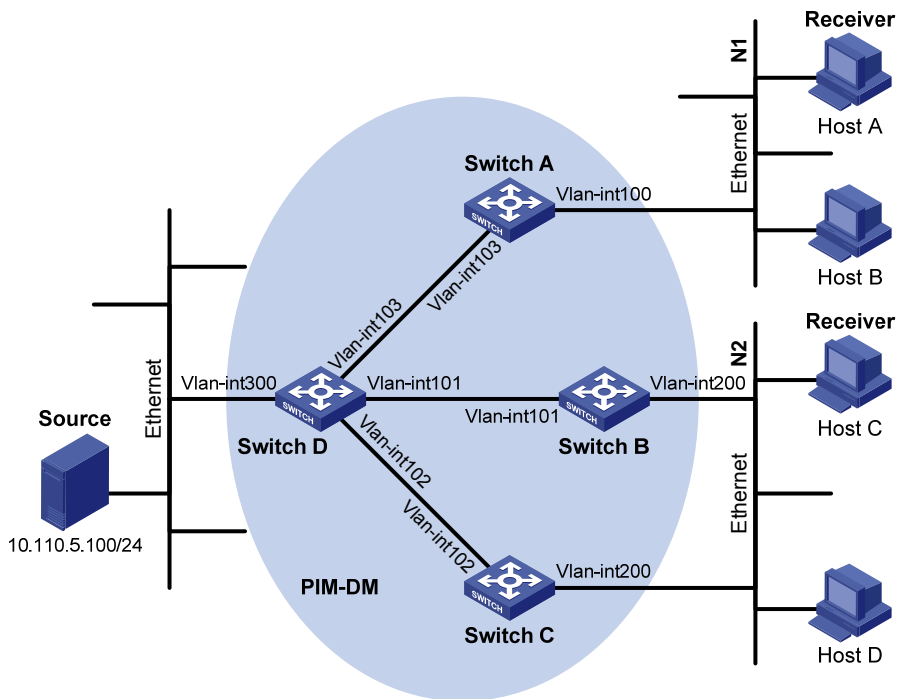
Network requirements

As shown in [Figure 53](#), receivers receive VOD information through multicast. The receiver groups of different organizations form stub networks, and one or more receiver hosts exist in each stub network. The entire PIM domain is operating in the dense mode.

Host A and Host C are multicast receivers in two stub networks.

IGMPv2 runs between Switch A and N1 and between Switch B/Switch C and N2.

Figure 53 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int100	10.110.1.1/24	Switch D	Vlan-int300	10.110.5.1/24
	Vlan-int103	192.168.1.1/24		Vlan-int103	192.168.1.2/24
Switch B	Vlan-int200	10.110.2.1/24		Vlan-int101	192.168.2.2/24
	Vlan-int101	192.168.2.1/24		Vlan-int102	192.168.3.2/24
Switch C	Vlan-int200	10.110.2.2/24			
	Vlan-int102	192.168.3.1/24			

Configuration procedure

1. Configure the IP address and subnet mask for each interface as per Figure 53. (Details not shown.)
2. Configure OSPF on the switches in the PIM-DM domain to make sure they are interoperable at the network layer. (Details not shown.)
3. Enable IP multicast routing, IGMP and PIM-DM:

Enable IP multicast routing on Switch A, enable IGMP on VLAN-interface 100, and enable PIM-DM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim dm
[SwitchA-Vlan-interface103] quit
```


#Enable IP multicast routing, IGMP and PIM-DM on Switch B and Switch C in the same way.
(Details not shown.)

Enable IP multicast routing on Switch D, and enable PIM-DM on each interface.

```
<SwitchD> system-view
[SwitchD] multicast routing-enable
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] pim dm
[SwitchD-Vlan-interface300] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim dm
[SwitchD-Vlan-interface103] quit
[SwitchD] interface vlan-interface 101
[SwitchD-Vlan-interface101] pim dm
[SwitchD-Vlan-interface101] quit
[SwitchD] interface vlan-interface 102
[SwitchD-Vlan-interface102] pim dm
[SwitchD-Vlan-interface102] quit
```

Verifying the configuration

Display PIM configuration information on Switch D.

```
[SwitchD] display pim interface
VPN-Instance: public net

Interface          NbrCnt HelloInt   DR-Pri   DR-Address
Vlan300            0       30         1        10.110.5.1   (local)
Vlan103            1       30         1        192.168.1.2  (local)
Vlan101            1       30         1        192.168.2.2  (local)
Vlan102            1       30         1        192.168.3.2  (local)
```

Display PIM neighboring relationships on Switch D.

```
[SwitchD] display pim neighbor
VPN-Instance: public net
Total Number of Neighbors = 3

Neighbor          Interface          Uptime   Expires   Dr-Priority
192.168.1.1       Vlan103            00:02:22 00:01:27 1
192.168.2.1       Vlan101            00:00:22 00:01:29 3
192.168.3.1       Vlan102            00:00:23 00:01:31 5
```

Assume that Host A needs to receive the information addressed to multicast group G 225.1.1.1. After multicast source S 10.110.5.100/24 sends multicast packets to the multicast group G, an SPT is established through traffic flooding. Switches on the SPT path (Switch A and Switch D) have their (S, G) entries. Host A sends an IGMP report to Switch A to join the multicast group G, and a (*, G) entry is generated on Switch A. You can use the **display pim routing-table** command to view the PIM routing table information on each switch. For example:

Display PIM routing table information on Switch A.

```
[SwitchA] display pim routing-table
VPN-Instance: public net
```

```

Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
  Protocol: pim-dm, Flag: WC
  UpTime: 00:04:25
  Upstream interface: NULL
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface100
      Protocol: igmp, UpTime: 00:04:25, Expires: never

(10.110.5.100, 225.1.1.1)
  Protocol: pim-dm, Flag: ACT
  UpTime: 00:06:14
  Upstream interface: Vlan-interface103
    Upstream neighbor: 192.168.1.2
    RPF prime neighbor: 192.168.1.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface100
      Protocol: pim-dm, UpTime: 00:04:25, Expires: never

```

Display PIM routing table information on Switch D.

```

[SwitchD] display pim routing-table
VPN-Instance: public net
Total 0 (*, G) entry; 1 (S, G) entry

(10.110.5.100, 225.1.1.1)
  Protocol: pim-dm, Flag: LOC ACT
  UpTime: 00:03:27
  Upstream interface: Vlan-interface300
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 2
    1: Vlan-interface103
      Protocol: pim-dm, UpTime: 00:03:27, Expires: never
    2: Vlan-interface102
      Protocol: pim-dm, UpTime: 00:03:27, Expires: never

```

PIM-SM non-scoped zone configuration example

Network requirements

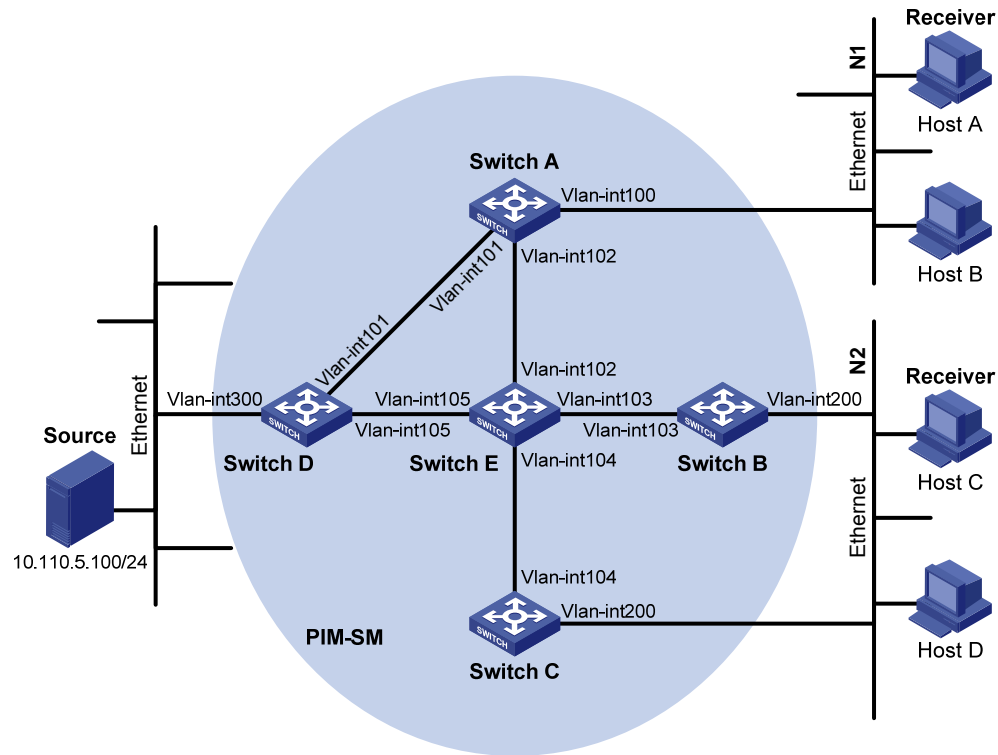
As shown in [Figure 54](#), receivers receive VOD information through multicast. The receiver groups of different organizations form stub networks, and one or more receiver hosts exist in each stub network. The entire PIM-SM domain contains only one BSR.

Host A and Host C are multicast receivers in two stub networks.

VLAN-interface 105 on Switch D and VLAN-interface 102 on Switch E act as C-BSRs and C-RPs. The C-BSR on Switch E has a higher priority. The multicast group range to which the C-RP is designated is 225.1.1.0/24. Modify the hash mask length to map a certain number of consecutive group addresses within the range to the two C-RPs.

IGMPv2 runs between Switch A and N1 and between Switch B/Switch C and N2.

Figure 54 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int100	10.110.1.1/24	Switch D	Vlan-int300	10.110.5.1/24
	Vlan-int101	192.168.1.1/24		Vlan-int101	192.168.1.2/24
	Vlan-int102	192.168.9.1/24		Vlan-int105	192.168.4.2/24
Switch B	Vlan-int200	10.110.2.1/24	Switch E	Vlan-int104	192.168.3.2/24
	Vlan-int103	192.168.2.1/24		Vlan-int103	192.168.2.2/24
Switch C	Vlan-int200	10.110.2.2/24		Vlan-int102	192.168.9.2/24
	Vlan-int104	192.168.3.1/24		Vlan-int105	192.168.4.1/24

Configuration procedure

1. Configure the IP address and subnet mask for each interface as per Figure 54. (Details not shown.)
2. Configure OSPF on the switches in the PIM-SM domain to make sure they are interoperable at the network layer. (Details not shown.)
3. Enable IP multicast routing, IGMP and PIM-SM:

Enable IP multicast routing on Switch A, enable IGMP on VLAN-interface 100, and enable PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim sm
[SwitchA-Vlan-interface102] quit
```

Enable IP multicast routing, IGMP and PIM-SM on Switch B and Switch C in the same way. (Details not shown.)

Enable IP multicast routing and PIM-SM on Switch D and Switch E in the same way. (Details not shown.)

4. Configure a C-BSR and a C-RP:

On Switch D, configure the service scope of RP, specify a C-BSR and a C-RP, and set the hash mask length to 32 and the priority of the C-BSR to 10.

```
<SwitchD> system-view
[SwitchD] acl number 2005
[SwitchD-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchD-acl-basic-2005] quit
[SwitchD] pim
[SwitchD-pim] c-bsr vlan-interface 105 32 10
[SwitchD-pim] c-rp vlan-interface 105 group-policy 2005
[SwitchD-pim] quit
```

On Switch E, configure the service scope of RP advertisements, specify a C-BSR and a C-RP, and set the hash mask length to 32 and the priority of the C-BSR to 20.

```
<SwitchE> system-view
[SwitchE] acl number 2005
[SwitchE-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchE-acl-basic-2005] quit
[SwitchE] pim
[SwitchE-pim] c-bsr vlan-interface 102 32 20
[SwitchE-pim] c-rp vlan-interface 102 group-policy 2005
[SwitchE-pim] quit
```

Verifying the configuration

Display PIM configuration information on Switch A.

```
[SwitchA] display pim interface
VPN-Instance: public net
Interface          NbrCnt HelloInt  DR-Pri  DR-Address
Vlan100            0        30       1       10.110.1.1 (local)
```

```
Vlan101          1      30      1      192.168.1.2
Vlan102          1      30      1      192.168.9.2
```

Display BSR information and the locally configured C-RP information in effect on Switch A.

```
[SwitchA] display pim bsr-info
VPN-Instance: public net
Elected BSR Address: 192.168.9.2
  Priority: 20
  Hash mask length: 32
  State: Accept Preferred
  Scope: Not scoped
  Uptime: 00:40:40
  Expires: 00:01:42
```

Display BSR information and the locally configured C-RP information in effect on Switch D.

```
[SwitchD] display pim bsr-info
VPN-Instance: public net
Elected BSR Address: 192.168.9.2
  Priority: 20
  Hash mask length: 32
  State: Accept Preferred
  Scope: Not scoped
  Uptime: 00:05:26
  Expires: 00:01:45
Candidate BSR Address: 192.168.4.2
  Priority: 10
  Hash mask length: 32
  State: Candidate
  Scope: Not scoped

Candidate RP: 192.168.4.2(Vlan-interface105)
  Priority: 192
  HoldTime: 150
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:34
```

Display BSR information and the locally configured C-RP information in effect on Switch E.

```
[SwitchE] display pim bsr-info
VPN-Instance: public net
Elected BSR Address: 192.168.9.2
  Priority: 20
  Hash mask length: 32
  State: Elected
  Scope: Not scoped
  Uptime: 00:01:18
  Next BSR message scheduled at: 00:01:52
Candidate BSR Address: 192.168.9.2
  Priority: 20
  Hash mask length: 32
  State: Elected
```

Scope: Not scoped

```
Candidate RP: 192.168.9.2(Vlan-interface102)
  Priority: 192
  HoldTime: 150
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:48
```

Display RP information on Switch A.

```
[SwitchA] display pim rp-info
VPN-Instance: public net
PIM-SM BSR RP information:
Group/MaskLen: 225.1.1.0/24
  RP: 192.168.4.2
  Priority: 192
  HoldTime: 150
  Uptime: 00:51:45
  Expires: 00:02:22

  RP: 192.168.9.2
  Priority: 192
  HoldTime: 150
  Uptime: 00:51:45
  Expires: 00:02:22
```

Assume that Host A needs to receive information addressed to the multicast group G 225.1.1.0. The RP corresponding to the multicast group G is Switch E as a result of hash calculation, so an RPT will be built between Switch A and Switch E. When the multicast source S 10.110.5.100/24 registers with the RP, an SPT will be built between Switch D and Switch E. After receiving multicast data, Switch A immediately switches from the RPT to the SPT. Switches on the RPT path (Switch A and Switch E) have a (*, G) entry, and switches on the SPT path (Switch A and Switch D) have an (S, G) entry. You can use the **display pim routing-table** command to view the PIM routing table information on the switches. For example:

Display PIM routing table information on Switch A.

```
[SwitchA] display pim routing-table
VPN-Instance: public net
Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.0)
  RP: 192.168.9.2
  Protocol: pim-sm, Flag: WC
  UpTime: 00:13:46
  Upstream interface: Vlan-interface102
    Upstream neighbor: 192.168.9.2
    RPF prime neighbor: 192.168.9.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface100
      Protocol: igmp, UpTime: 00:13:46, Expires: 00:03:06
```

```
(10.110.5.100, 225.1.1.0)
  RP: 192.168.9.2
  Protocol: pim-sm, Flag: SPT ACT
  UpTime: 00:00:42
  Upstream interface: Vlan-interface101
    Upstream neighbor: 192.168.1.2
    RPF prime neighbor: 192.168.1.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface100
      Protocol: pim-sm, UpTime: 00:00:42, Expires: 00:03:06
```

The information on Switch B and Switch C is similar to that on Switch A.

Display PIM routing table information on Switch D.

```
[SwitchD] display pim routing-table
VPN-Instance: public net
Total 0 (*, G) entry; 1 (S, G) entry
```

```
(10.110.5.100, 225.1.1.0)
  RP: 192.168.9.2
  Protocol: pim-sm, Flag: SPT LOC ACT
  UpTime: 00:00:42
  Upstream interface: Vlan-interface300
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface105
      Protocol: pim-sm, UpTime: 00:00:42, Expires: 00:02:26
```

Display PIM routing table information on Switch E.

```
[SwitchE] display pim routing-table
VPN-Instance: public net
Total 1 (*, G) entry; 0 (S, G) entry
```

```
(*, 225.1.1.0)
  RP: 192.168.9.2 (local)
  Protocol: pim-sm, Flag: WC
  UpTime: 00:13:16
  Upstream interface: Register
    Upstream neighbor: 192.168.4.2
    RPF prime neighbor: 192.168.4.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface102
      Protocol: pim-sm, UpTime: 00:13:16, Expires: 00:03:22
```

PIM-SM admin-scope zone configuration example

Network requirements

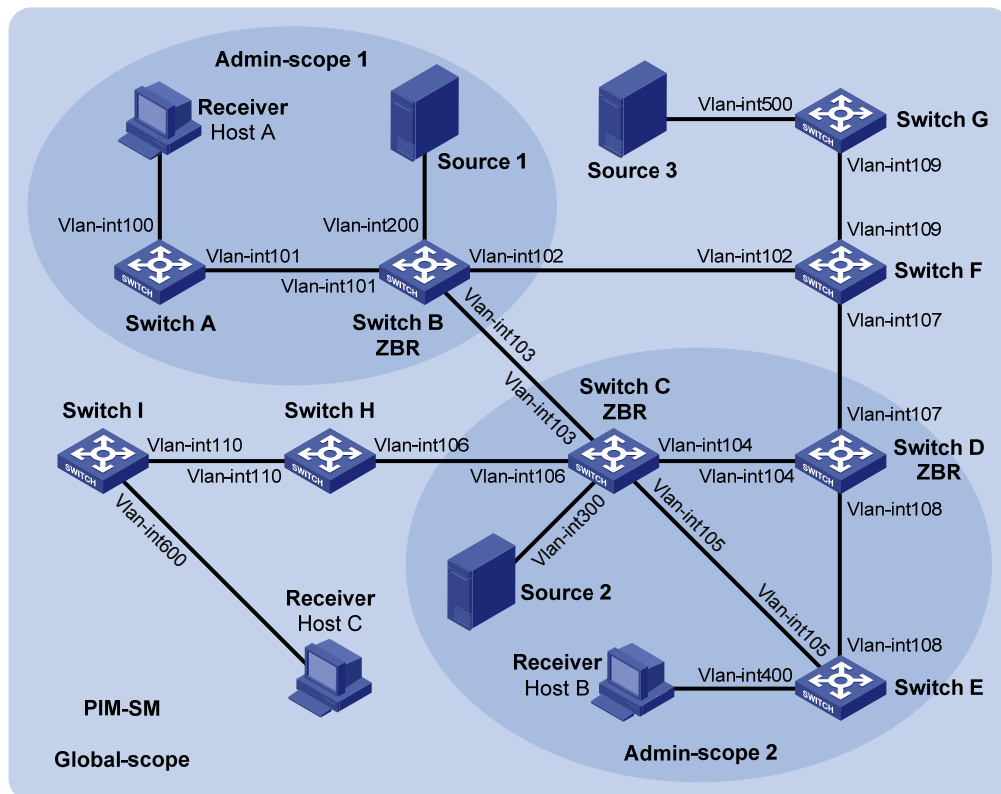
As shown in [Figure 55](#), receivers receive VOD information through multicast. The entire PIM-SM domain is divided into admin-scope zone 1, admin-scope zone 2, and the global zone. Switch B, Switch C, and Switch D are ZBRs of these three domains respectively.

Source 1 and Source 2 send different multicast information to multicast group 239.1.1.1. Host A receives the multicast information only from Source 1, and Host B receives the multicast information only from Source 2. Source 3 sends multicast information to multicast group 224.1.1.1. Host C is a multicast receiver for this multicast group.

VLAN-interface 101 of Switch B acts as a C-BSR and C-RP of admin-scope zone 1, which provides services for the multicast group range 239.0.0.0/8. VLAN-interface 104 of Switch D acts as a C-BSR and C-RP of admin-scope zone 2, which also provides services for the multicast group range 239.0.0.0/8. VLAN-interface 109 of Switch F acts as C-BSRs and C-RPs of the global scope zone, which provides services for all the multicast groups other than those in the 239.0.0.0/8 range.

IGMPv2 runs between Switch A, Switch E, Switch I, and their respective receivers.

Figure 55 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int100	192.168.1.1/24	Switch D	Vlan-int104	10.110.4.2/24
	Vlan-int101	10.110.1.1/24		Vlan-int108	10.110.7.1/24
Switch B	Vlan-int200	192.168.2.1/24	Switch E	Vlan-int400	192.168.4.1/24
	Vlan-int101	10.110.1.2/24		Vlan-int105	10.110.5.2/24
	Vlan-int103	10.110.2.1/24	Switch F	Vlan-int108	10.110.7.2/24
	Vlan-int102	10.110.3.1/24		Vlan-int102	10.110.3.2/24
Switch C	Vlan-int300	192.168.3.1/24	Switch G	Vlan-int500	192.168.5.1/24
	Vlan-int104	10.110.4.1/24		Vlan-int109	10.110.9.2/24
	Vlan-int105	10.110.5.1/24	Source 1	—	192.168.2.10/24
	Vlan-int103	10.110.2.2/24		Source 2	—
Switch H	Vlan-int110	10.110.10.1/24	Source 3		—
	Vlan-int106	10.110.6.2/24			
Switch I	Vlan-int600	192.168.6.1/24			
	Vlan-int110	10.110.10.2/24			

Configuration procedure

1. Configure the IP address and subnet mask for each interface as per Figure 55. (Details not shown.)
2. Configure OSPF on the switches in the PIM-SM domain to make sure they are interoperable at the network layer. (Details not shown.)
3. Enable IP multicast routing and administrative scoping, and enable IGMP and PIM-SM:

Enable IP multicast routing and administrative scoping on Switch A, enable IGMP on VLAN-interface 100, and enable PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] pim
[SwitchA-pim] c-bsr admin-scope
[SwitchA-pim] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
```

Enable IP multicast routing and administrative scoping, and enable IGMP and PIM-SM on Switch E and Switch I in the same way. (Details not shown.)

On Switch B, enable IP multicast routing and administrative scoping, and enable PIM-SM on each interface.

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] pim
[SwitchB-pim] c-bsr admin-scope
[SwitchB-pim] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] pim sm
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim sm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim sm
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] pim sm
[SwitchB-Vlan-interface103] quit
```

Enable IP multicast routing and administrative scoping, and enable PIM-SM on Switch C, Switch D, Switch F, Switch G, and Switch H in the same way. (Details not shown.)

4. Configure an admin-scope zone boundary:

On Switch B, configure VLAN-interface 102 and VLAN-interface 103 to be the boundary of admin-scope zone 1.

```
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] multicast boundary 239.0.0.0 8
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] multicast boundary 239.0.0.0 8
[SwitchB-Vlan-interface103] quit
```

On Switch C, configure VLAN-interface 103 and VLAN-interface 106 to be the boundary of admin-scope zone 2.

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 103
[SwitchC-Vlan-interface103] multicast boundary 239.0.0.0 8
[SwitchC-Vlan-interface103] quit
[SwitchC] interface vlan-interface 106
[SwitchC-Vlan-interface106] multicast boundary 239.0.0.0 8
[SwitchC-Vlan-interface106] quit
```

On Switch D, configure VLAN-interface 107 to be the boundary of admin-scope zone 2.

```
<SwitchD> system-view
[SwitchD] interface vlan-interface 107
[SwitchD-Vlan-interface107] multicast boundary 239.0.0.0 8
[SwitchD-Vlan-interface107] quit
```

5. Configure C-BSRs and C-RPs:

On Switch B, configure the service scope of RP advertisements, and configure VLAN-interface 101 as a C-BSR and C-RP of admin-scope zone 1.

```
[SwitchB] acl number 2001
[SwitchB-acl-basic-2001] rule permit source 239.0.0.0 0.255.255.255
[SwitchB-acl-basic-2001] quit
[SwitchB] pim
[SwitchB-pim] c-bsr group 239.0.0.0 8
[SwitchB-pim] c-bsr vlan-interface 101
[SwitchB-pim] c-rp vlan-interface 101 group-policy 2001
[SwitchB-pim] quit
```

On Switch D, configure the service scope of RP advertisements, and configure VLAN-interface 104 as a C-BSR and C-RP of admin-scope zone 2.

```
[SwitchD] acl number 2001
[SwitchD-acl-basic-2001] rule permit source 239.0.0.0 0.255.255.255
[SwitchD-acl-basic-2001] quit
[SwitchD] pim
[SwitchD-pim] c-bsr group 239.0.0.0 8
[SwitchD-pim] c-bsr vlan-interface 104
[SwitchD-pim] c-rp vlan-interface 104 group-policy 2001
[SwitchD-pim] quit
```

On Switch F, configure VLAN-interface 109 as a C-BSR and C-RP in the global scope zone.

```
<SwitchF> system-view
[SwitchF] pim
[SwitchF-pim] c-bsr global
[SwitchF-pim] c-bsr vlan-interface 109
[SwitchF-pim] c-rp vlan-interface 109
[SwitchF-pim] quit
```

Verifying the configuration

Display BSR information and the locally configured C-RP information on Switch B.

```
[SwitchB] display pim bsr-info
```

```
VPN-Instance: public net
Elected BSR Address: 10.110.9.1
  Priority: 64
  Hash mask length: 30
  State: Accept Preferred
  Scope: Global
  Uptime: 00:01:45
  Expires: 00:01:25
Elected BSR Address: 10.110.1.2
  Priority: 64
  Hash mask length: 30
  State: Elected
  Scope: 239.0.0.0/8
  Uptime: 00:04:54
  Next BSR message scheduled at: 00:00:06
Candidate BSR Address: 10.110.1.2
  Priority: 64
  Hash mask length: 30
  State: Elected
  Scope: 239.0.0.0/8

Candidate RP: 10.110.1.2(Vlan-interface101)
  Priority: 192
  HoldTime: 150
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:15
```

Display BSR information and the locally configured C-RP information on Switch D.

```
[SwitchD] display pim bsr-info
VPN-Instance: public net
Elected BSR Address: 10.110.9.1
  Priority: 64
  Hash mask length: 30
  State: Accept Preferred
  Scope: Global
  Uptime: 00:01:45
  Expires: 00:01:25
Elected BSR Address: 10.110.4.2
  Priority: 64
  Hash mask length: 30
  State: Elected
  Scope: 239.0.0.0/8
  Uptime: 00:03:48
  Next BSR message scheduled at: 00:01:12
Candidate BSR Address: 10.110.4.2
  Priority: 64
  Hash mask length: 30
  State: Elected
  Scope: 239.0.0.0/8
```

```
Candidate RP: 10.110.4.2(Vlan-interface104)
  Priority: 192
  HoldTime: 150
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:10
```

Display BSR information and the locally configured C-RP information on Switch F.

```
[SwitchF] display pim bsr-info
VPN-Instance: public net
Elected BSR Address: 10.110.9.1
  Priority: 64
  Hash mask length: 30
  State: Elected
  Scope: Global
  Uptime: 00:11:11
  Next BSR message scheduled at: 00:00:49
Candidate BSR Address: 10.110.9.1
  Priority: 64
  Hash mask length: 30
  State: Elected
  Scope: Global
```

```
Candidate RP: 10.110.9.1(Vlan-interface109)
  Priority: 192
  HoldTime: 150
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:55
```

Display RP information on Switch B.

```
[SwitchB] display pim rp-info
VPN-Instance: public net
PIM-SM BSR RP information:
Group/MaskLen: 224.0.0.0/4
  RP: 10.110.9.1
  Priority: 192
  HoldTime: 150
  Uptime: 00:03:39
  Expires: 00:01:51
```

```
Group/MaskLen: 239.0.0.0/8
  RP: 10.110.1.2 (local)
  Priority: 192
  HoldTime: 150
  Uptime: 00:07:44
  Expires: 00:01:51
```

Display RP information on Switch D.

```
[SwitchD] display pim rp-info
VPN-Instance: public net
```

```
PIM-SM BSR RP information:
Group/MaskLen: 224.0.0.0/4
  RP: 10.110.9.1
  Priority: 192
  HoldTime: 150
  Uptime: 00:03:42
  Expires: 00:01:48
```

```
Group/MaskLen: 239.0.0.0/8
  RP: 10.110.4.2 (local)
  Priority: 192
  HoldTime: 150
  Uptime: 00:06:54
  Expires: 00:02:41
```

Display RP information on Switch F.

```
[SwitchF] display pim rp-info
VPN-Instance: public net
PIM-SM BSR RP information:
Group/MaskLen: 224.0.0.0/4
  RP: 10.110.9.1 (local)
  Priority: 192
  HoldTime: 150
  Uptime: 00:00:32
  Expires: 00:01:58
```

BIDIR-PIM configuration example

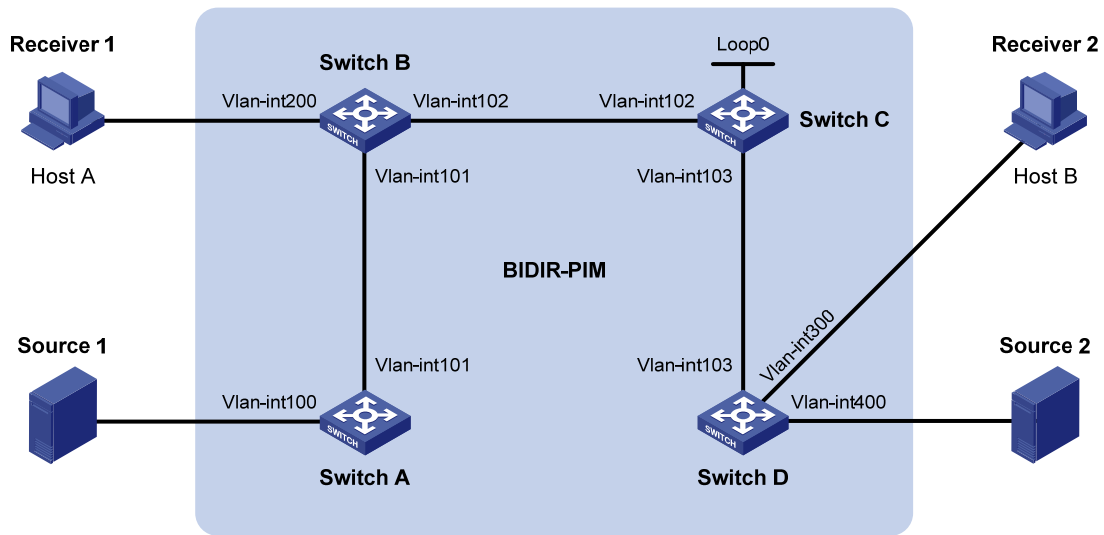
Network requirements

In the BIDIR-PIM domain shown in [Figure 56](#). Source 1 and Source 2 send different multicast information to multicast group 225.1.1.1. Host A and Host B receive multicast information from the two sources.

VLAN interface 102 of Switch C acts as a C-BSR, and loopback interface 0 of Switch C acts as a C-RP of the BIDIR-PIM domain.

IGMPv2 runs between Switch B and Host A, and between Switch D and Host B.

Figure 56 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int100	192.168.1.1/24	Switch D	Vlan-int300	192.168.3.1/24
	Vlan-int101	10.110.1.1/24		Vlan-int400	192.168.4.1/24
Switch B	Vlan-int200	192.168.2.1/24		Vlan-int103	10.110.3.2/24
	Vlan-int101	10.110.1.2/24	Source 1	-	192.168.1.100/24
	Vlan-int102	10.110.2.1/24	Source 2	-	192.168.4.100/24
Switch C	Vlan-int102	10.110.2.2/24	Receiver 1	-	192.168.2.100/24
	Vlan-int103	10.110.3.1/24	Receiver 2	-	192.168.3.100/24
	Loop0	1.1.1.1/32			

Configuration procedure

1. Configure an IP address and subnet mask for each interface as per Figure 56. (Details not shown.)
2. Configure OSPF on the switches in the BIDIR-PIM domain to make sure they are interoperable at the network layer. (Details not shown.)
3. Enable IP multicast routing, PIM-SM, BIDIR-PIM, and IGMP:

On Switch A, enable IP multicast routing, enable PIM-SM on each interface, and enable BIDIR-PIM.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] pim
[SwitchA-pim] bidir-pim enable
[SwitchA-pim] quit
```

On Switch B, enable IP multicast routing, enable PIM-SM on each interface, enable IGMP in VLAN interface 200, and enable BIDIR-PIM.

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
[SwitchB-Vlan-interface200] pim sm
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim sm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim sm
[SwitchB-Vlan-interface102] quit
[SwitchB] pim
[SwitchB-pim] bidir-pim enable
[SwitchB-pim] quit
```

On Switch C, enable IP multicast routing, enable PIM-SM on each interface, and enable BIDIR-PIM.

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 102
[SwitchC-Vlan-interface102] pim sm
[SwitchC-Vlan-interface102] quit
[SwitchC] interface vlan-interface 103
[SwitchC-Vlan-interface103] pim sm
[SwitchC-Vlan-interface103] quit
[SwitchC] interface loopback 0
[SwitchC-LoopBack0] pim sm
[SwitchC-LoopBack0] quit
[SwitchC] pim
[SwitchC-pim] bidir-pim enable
```

On Switch D, enable IP multicast routing, enable PIM-SM on each interface, enable IGMP in VLAN interface 300, and enable BIDIR-PIM.

```
<SwitchD> system-view
[SwitchD] multicast routing-enable
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] igmp enable
[SwitchD-Vlan-interface300] pim sm
[SwitchD-Vlan-interface300] quit
[SwitchD] interface vlan-interface 400
[SwitchD-Vlan-interface400] pim sm
[SwitchD-Vlan-interface400] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim sm
[SwitchD-Vlan-interface103] quit
[SwitchD] pim
```



```
[SwitchD-pim] bidir-pim enable
[SwitchD-pim] quit
```

4. On Switch C, configure VLAN interface 102 as a C-BSR, and loopback interface 0 as a C-RP for the entire BIDIR-PIM domain.

```
[SwitchC-pim] c-bsr vlan-interface 102
[SwitchC-pim] c-rp loopback 0 bidir
[SwitchC-pim] quit
```

Verifying the configuration

- # Display the DF information of BIDIR-PIM on Switch A.

```
[SwitchA] display pim df-info
VPN-Instance: public net
```

```
RP Address: 1.1.1.1
```

Interface	State	DF-Pref	DF-Metric	DF-Uptime	DF-Address
Vlan100	Win	100	2	01:08:50	192.168.1.1 (local)
Vlan101	Lose	100	1	01:07:49	10.110.1.2

- # Display the DF information of BIDIR-PIM on Switch B.

```
[SwitchB] display pim df-info
VPN-Instance: public net
```

```
RP Address: 1.1.1.1
```

Interface	State	DF-Pref	DF-Metric	DF-Uptime	DF-Address
Vlan200	Win	100	1	01:24:09	192.168.2.1 (local)
Vlan101	Win	100	1	01:24:09	10.110.1.2 (local)
Vlan102	Lose	0	0	01:23:12	10.110.2.2

- # Display the DF information of BIDIR-PIM on Switch C.

```
[SwitchC] display pim df-info
VPN-Instance: public net
```

```
RP Address: 1.1.1.1
```

Interface	State	DF-Pref	DF-Metric	DF-Uptime	DF-Address
Loop0	-	-	-	-	-
Vlan102	Win	0	0	01:06:07	10.110.2.2 (local)
Vlan103	Win	0	0	01:06:07	10.110.3.1 (local)

- # Display the DF information of BIDIR-PIM on Switch D.

```
[SwitchD] display pim df-info
VPN-Instance: public net
```

```
RP Address: 1.1.1.1
```

Interface	State	DF-Pref	DF-Metric	DF-Uptime	DF-Address
Vlan300	Win	100	1	01:19:53	192.168.3.1 (local)
Vlan400	Win	100	1	00:39:34	192.168.4.1 (local)
Vlan103	Lose	0	0	01:21:40	10.110.3.1

- # Display the DF information of the multicast forwarding table on Switch A.

```
[SwitchA] display multicast forwarding-table df-info
```

```
Multicast DF information of VPN-Instance: public net
Total 1 RP
```

```
Total 1 RP matched
```

```
00001. RP Address: 1.1.1.1
MID: 0, Flags: 0x2100000:0
Uptime: 00:08:32
RPF interface: Vlan-interface101
List of 1 DF interfaces:
  1: Vlan-interface100
```

Display the DF information of the multicast forwarding table on Switch B.

```
[SwitchB] display multicast forwarding-table df-info
Multicast DF information of VPN-Instance: public net
Total 1 RP
```

```
Total 1 RP matched
```

```
00001. RP Address: 1.1.1.1
MID: 0, Flags: 0x2100000:0
Uptime: 00:06:24
RPF interface: Vlan-interface102
List of 2 DF interfaces:
  1: Vlan-interface101
  2: Vlan-interface200
```

Display the DF information of the multicast forwarding table on Switch C.

```
[SwitchC] display multicast forwarding-table df-info
Multicast DF information of VPN-Instance: public net
Total 1 RP
```

```
Total 1 RP matched
```

```
00001. RP Address: 1.1.1.1
MID: 0, Flags: 0x2100000:0
Uptime: 00:07:21
RPF interface: LoopBack0
List of 2 DF interfaces:
  1: Vlan-interface102
  2: Vlan-interface103
```

Display the DF information of the multicast forwarding table on Switch D.

```
[SwitchD] display multicast forwarding-table df-info
Multicast DF information of VPN-Instance: public net
Total 1 RP
```

```
Total 1 RP matched
```

```
00001. RP Address: 1.1.1.1
```

```

MID: 0, Flags: 0x2100000:0
Uptime: 00:05:12
RPF interface: Vlan-interface103
List of 2 DF interfaces:
  1: Vlan-interface300
  2: Vlan-interface400

```

PIM-SSM configuration example

Network requirements

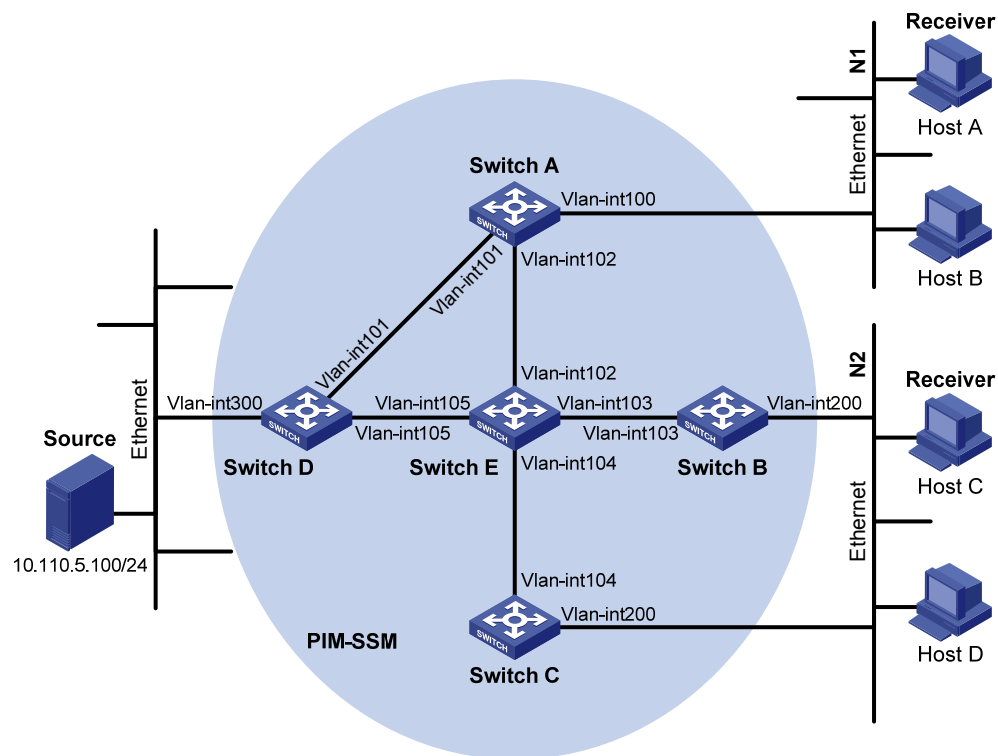
As shown in [Figure 57](#), receivers receive VOD information through multicast. The receiver groups of different organizations form stub networks, and one or more receiver hosts exist in each stub network. The entire PIM domain is operating in the SSM mode.

Host A and Host C are multicast receivers in two stub networks.

The SSM group range is 232.1.1.0/24.

IGMPv3 runs between Switch A and N1 and between Switch B/Switch C and N2.

Figure 57 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int100	10.110.1.1/24	Switch D	Vlan-int300	10.110.5.1/24
	Vlan-int101	192.168.1.1/24		Vlan-int101	192.168.1.2/24
	Vlan-int102	192.168.9.1/24		Vlan-int105	192.168.4.2/24
Switch B	Vlan-int200	10.110.2.1/24	Switch E	Vlan-int104	192.168.3.2/24

	Vlan-int103	192.168.2.1/24	Vlan-int103	192.168.2.2/24
Switch C	Vlan-int200	10.110.2.2/24	Vlan-int102	192.168.9.2/24
	Vlan-int104	192.168.3.1/24	Vlan-int105	192.168.4.1/24

Configuration procedure

1. Configure the IP address and subnet mask for each interface as per [Figure 57](#). (Details not shown.)
2. Configure OSPF on the switches in the PIM-SSM domain to make sure they are interoperable at the network layer. (Details not shown.)
3. Enable IP multicast routing, IGMP and PIM-SM:

Enable IP multicast routing on Switch A, enable IGMPv3 on VLAN-interface 100, and enable PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] igmp version 3
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim sm
[SwitchA-Vlan-interface102] quit
```

Enable IP multicast routing, IGMP and PIM-SM on Switch B and Switch C in the same way. (Details not shown.)

Enable IP multicast routing and PIM-SM on Switch D and Switch E in the same way. (Details not shown.)

4. Configure the SSM group range:

Configure the SSM group range to be 232.1.1.0/24 on Switch A.

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
[SwitchA] pim
[SwitchA-pim] ssm-policy 2000
[SwitchA-pim] quit
```

Configure the SSM group range on Switch B, Switch C, Switch D and Switch E in the same way. (Details not shown.)

Verifying the configuration

Display PIM configuration information on Switch A.

```
[SwitchA] display pim interface
VPN-Instance: public net
Interface          NbrCnt HelloInt  DR-Pri  DR-Address
```

Vlan100	0	30	1	10.110.1.1	(local)
Vlan101	1	30	1	192.168.1.2	
Vlan102	1	30	1	192.168.9.2	

Assume that Host A needs to receive the information a specific multicast source S 10.110.5.100/24 sends to multicast group G 232.1.1.1. Switch A builds an SPT toward the multicast source. Switches on the SPT path (Switch A and Switch D) have generated an (S, G) entry, but Switch E, which is not on the SPT path, does not have multicast routing entries. You can use the **display pim routing-table** command to view the PIM routing table information on each switch. For example:

Display PIM routing table information on Switch A.

```
[SwitchA] display pim routing-table
VPN-Instance: public net
Total 0 (*, G) entry; 1 (S, G) entry

(10.110.5.100, 232.1.1.1)
  Protocol: pim-ssm, Flag:
  UpTime: 00:13:25
  Upstream interface: Vlan-interface101
    Upstream neighbor: 192.168.1.2
    RPF prime neighbor: 192.168.1.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface100
      Protocol: igmp, UpTime: 00:13:25, Expires: 00:03:25
```

Display PIM routing table information on Switch D.

```
[SwitchD] display pim routing-table
VPN-Instance: public net
Total 0 (*, G) entry; 1 (S, G) entry

(10.110.5.100, 232.1.1.1)
  Protocol: pim-ssm, Flag: LOC
  UpTime: 00:12:05
  Upstream interface: Vlan-interface300
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface105
      Protocol: pim-ssm, UpTime: 00:12:05, Expires: 00:03:25
```

Troubleshooting PIM

A multicast distribution tree cannot be built correctly

Symptom

None of the routers in the network (including routers directly connected with multicast sources and receivers) have multicast forwarding entries. That is, a multicast distribution tree cannot be built correctly and clients cannot receive multicast data.

Analysis

- When PIM-DM runs on the entire network, multicast data is flooded from the first hop router connected with the multicast source to the last hop router connected with the clients. When the multicast data is flooded to a router, regardless of which router it is, the router creates (S, G) entries only if it has a route to the multicast source. If the router does not have a route to the multicast source, or if PIM-DM is not enabled on the router's RPF interface to the multicast source, the router cannot create (S, G) entries.
- When PIM-SM runs on the entire network and when a router will join the SPT, the router creates (S, G) entries only if it has a route to the multicast source. If the router does not have a route to the multicast source, or if PIM-DM is not enabled on the router's RPF interface to the multicast source, the router cannot create (S, G) entries.
- When a multicast router receives a multicast packet, it searches the existing unicast routing table for the optimal route to the RPF check object. The outgoing interface of this route will act as the RPF interface and the next hop will be taken as the RPF neighbor. The RPF interface completely relies on the existing unicast route, and is independent of PIM. The RPF interface must be PIM-enabled, and the RPF neighbor must also be a PIM neighbor. If PIM is not enabled on the router where the RPF interface or the RPF neighbor resides, the establishment of a multicast distribution tree will surely fail, causing abnormal multicast forwarding.
- Because a hello message does not carry the PIM mode information, a router that is running PIM cannot identify what PIM mode its PIM neighbor is running. If different PIM modes are enabled on the RPF interface and on the corresponding interface of the RPF neighbor router, the establishment of a multicast distribution tree will fail, causing abnormal multicast forwarding.
- The same PIM mode must run on the entire network. Otherwise, the establishment of a multicast distribution tree will fail, causing abnormal multicast forwarding.

Solution

1. Use the **display ip routing-table** command to verify that a unicast route exists from the receiver host to the multicast source.
2. Use the **display pim interface** command to verify that PIM is enabled on the interfaces, especially on the RPF interface. If PIM is not enabled on the interface, use the **pim dm** or **pim sm** command to enable PIM-DM or PIM-SM.
3. Use the **display pim neighbor** command to verify that the RPF neighbor is a PIM neighbor.

4. Verify that PIM and IGMP are enabled on the interfaces directly connecting to the multicast source and to the receivers.
5. Use the **display pim interface verbose** command to verify that the same PIM mode is enabled on the RPF interface and the corresponding interface of the RPF neighbor router.
6. Verify that the same PIM mode is enabled on all the routers in the entire network. Make sure that the same PIM mode is enabled on all the routers: PIM-SM on all routers, or PIM-DM on all routers. In the case of PIM-SM, also check that the BSR and RP configurations are correct.

Multicast data abnormally terminated on an intermediate router

Symptom

An intermediate router can receive multicast data successfully, but the data cannot reach the last hop router. An interface on the intermediate router receives data but no corresponding (S, G) entry is created in the PIM routing table.

Analysis

- If a multicast forwarding boundary has been configured through the **multicast boundary** command, any multicast packet will be kept from crossing the boundary, and no routing entry can be created in the PIM routing table.
- In addition, the **source-policy** command filters received multicast packets. If the multicast data fails to pass the ACL rule defined in this command, PIM cannot create the route entry either.

Solution

1. Use the **display current-configuration** command to verify the multicast forwarding boundary settings. Use the **multicast boundary** command to change the multicast forwarding boundary settings.
2. Use the **display current-configuration** command to verify the multicast filter configuration. Change the ACL rule defined in the **source-policy** command so that the source/group address of the multicast data can pass ACL filtering.

RPs cannot join SPT in PIM-SM

Symptom

An RPT cannot be established correctly, or the RPs cannot join the SPT to the multicast source.

Analysis

- As the core of a PIM-SM domain, the RPs provide services for specific multicast groups. Multiple RPs can coexist in a network. Make sure that the RP information on all routers is exactly the same and that a specific group is mapped to the same RP. Otherwise, multicast forwarding will fail.

- If the static RP mechanism is used, the same static RP command must be executed on all the routers in the entire network. Otherwise, multicast forwarding will fail.

Solution

1. Use the **display ip routing-table** command to verify that a route is available on each router to the RP.
2. Use the **display pim rp-info** command to verify that the RP information is consistent on all routers.
3. Use the **display pim rp-info** command to verify that the same static RP address has been configured on all the routers in the entire network.

RPT establishment failure or source registration failure in PIM-SM

Symptom

C-RPs cannot unicast advertise messages to the BSR. The BSR does not advertise bootstrap messages containing C-RP information and has no unicast route to any C-RP. An RPT cannot be established correctly, or the DR cannot perform source registration with the RP.

Analysis

- The C-RPs periodically send C-RP-Adv messages to the BSR by unicast. If a C-RP has no unicast route to the BSR, the BSR cannot receive C-RP-Adv messages from that C-RP and the bootstrap message of the BSR will not contain the information of that C-RP.
- In addition, if the BSR does not have a unicast route to a C-RP, it will discard the C-RP-Adv messages from that C-RP, and therefore the bootstrap messages of the BSR will not contain the information of that C-RP.
- The RP is the core of a PIM-SM domain. Make sure that the RP information on all routers is exactly the same, a specific group G is mapped to the same RP, and unicast routes are available to the RP.

Solution

1. Use the **display ip routing-table** command to verify that routes are available on each router to the RP and the BSR and whether a route is available between the RP and the BSR. Make sure that each C-RP has a unicast route to the BSR, the BSR has a unicast route to each C-RP, and all the routers in the entire network have a unicast route to the RP.
2. PIM-SM needs the support of the RP and BSR. Use the **display pim bsr-info** command to verify that the BSR information is available on each router, and then use the **display pim rp-info** command to verify that the RP information is correct.
3. Use the **display pim neighbor** command to verify that the normal PIM neighboring relationships have been established among the routers.

Configuring MSDP (available only on the HP 5500 EI)

Overview

Multicast source discovery protocol (MSDP) is an inter-domain multicast solution that addresses the interconnection of protocol independent multicast sparse mode (PIM-SM) domains. You can use it to discover multicast source information in other PIM-SM domains.

In the basic PIM-SM mode, a multicast source registers only with the RP in the local PIM-SM domain, and the multicast source information about a domain is isolated from that of another domain. As a result, the RP obtains the source information only within the local domain, and a multicast distribution tree is built only within the local domain to deliver multicast data from a local multicast source to local receivers. MSDP enables the RPs of different PIM-SM domains to share their multicast source information, so that the local RP can join multicast sources in other domains, and multicast data can be transmitted among different domains.

With MSDP peer relationship established between appropriate routers in the network, the RPs of different PIM-SM domains are interconnected with one another. These MSDP peers exchange source active (SA) messages, so that the multicast source information is shared among these different domains.

NOTE:

- MSDP is applicable only if the intra-domain multicast protocol is PIM-SM.
 - MSDP is meaningful only for the any-source multicast (ASM) model.
-

For more information about the concepts of designated router (DR), bootstrap router (BSR), candidate-BSR (C-BSR), rendezvous point (RP), candidate-RP (C-RP), shortest path tree (SPT) and rendezvous point tree (RPT) mentioned in this document, see "[Configuring PIM \(available only on the HP 5500 EI\)](#)."

The term "router" in this document refers to both routers and Layer 3 switches.

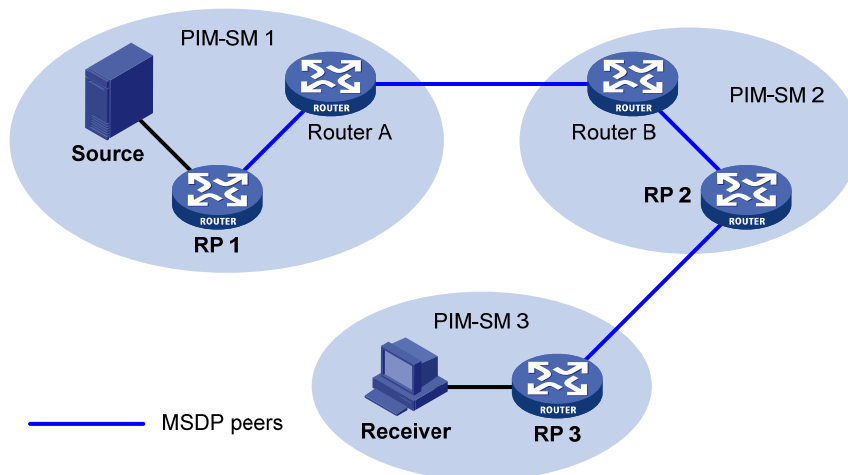
The term "interface" in this chapter collectively refers to Layer 3 interfaces, including VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

How MSDP works

MSDP peers

Configuring one or more pairs of MSDP peers in the network forms an MSDP interconnection map, where the RPs of different PIM-SM domains are interconnected in series. An SA message that an RP sends and that these MSDP peers relay can be delivered to all other RPs.

Figure 58 Where MSDP peers are in the network



As shown in [Figure 58](#), an MSDP peer can be created on any PIM-SM router. MSDP peers created on PIM-SM routers that assume different roles function differently.

1. MSDP peers on RPs include the following types:
 - **Source-side MSDP peer**—The MSDP peer nearest to the multicast source (Source), typically the source-side RP, like RP 1. The source-side RP creates SA messages and sends the messages to its remote MSDP peer to notify the MSDP peer of the locally registered multicast source information. A source-side MSDP peer must be created on the source-side RP. Otherwise it will not be able to advertise the multicast source information out of the PIM-SM domain.
 - **Receiver-side MSDP peer**—The MSDP peer nearest to the receivers, typically the receiver-side RP, like RP 3. After receiving an SA message, the receiver-side MSDP peer resolves the multicast source information carried in the message and joins the SPT rooted at the source across the PIM-SM domain. When multicast data from the multicast source arrives, the receiver-side MSDP peer forwards the data to the receivers along the RPT.
 - **Intermediate MSDP peer**—An MSDP peer with multicast remote MSDP peers, like RP 2. An intermediate MSDP peer forwards SA messages received from one remote MSDP peer to other remote MSDP peers, functioning as a relay of multicast source information.
2. MSDP peers created on common PIM-SM routers (other than RPs)

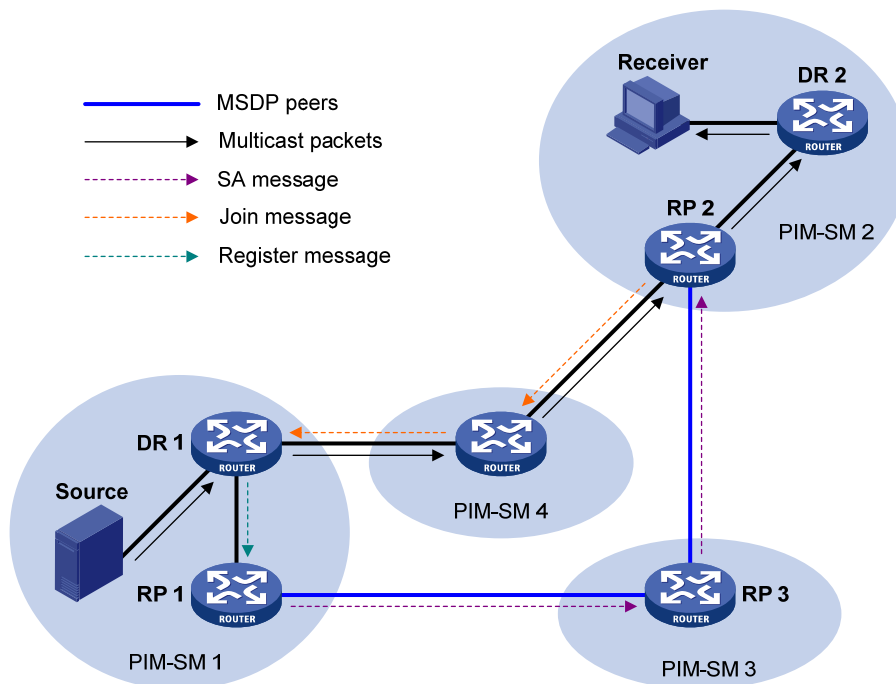
Router A and Router B are MSDP peers on common multicast routers. Such MSDP peers just forward received SA messages.

In a PIM-SM network running the BSR mechanism, the RP is dynamically elected from C-RPs. To enhance network robustness, a PIM-SM network typically has more than one C-RP. As the RP election result is unpredictable, MSDP peering relationship must be built among all C-RPs so that the winner C-RP is always on the "MSDP interconnection map," and loser C-RPs will assume the role of common PIM-SM routers on the "MSDP interconnection map."

Inter-domain multicast delivery through MSDP

As shown in Figure 59, an active source (Source) exists in the domain PIM-SM 1, and RP 1 has learned the existence of Source through multicast source registration. If RPs in PIM-SM 2 and PIM-SM 3 also seek the specific location of Source so that receiver hosts can receive multicast traffic that the source sends, HP recommends you to establish MSDP peering relationship between RP 1 and RP 3 and between RP 3 and RP 2, respectively.

Figure 59 Inter-domain multicast delivery through MSDP



The process of implementing PIM-SM inter-domain multicast delivery by leveraging MSDP peers is as follows:

1. When the multicast source in PIM-SM 1 sends the first multicast packet to multicast group G, DR 1 encapsulates the multicast data within a register message and sends the register message to RP 1. Then, RP 1 identifies the information related to the multicast source.
2. As the source-side RP, RP 1 creates SA messages and periodically sends the SA messages to its MSDP peer. An SA message contains the source address (S), the multicast group address (G), and the address of the RP that has created this SA message (namely, RP 1).
3. On MSDP peers, each SA message undergoes a reverse path forwarding (RPF) check and multicast policy-based filtering, so that only SA messages that have arrived along the correct path and passed the filtering are received and forwarded. This avoids delivery loops of SA messages.

In addition, you can configure MSDP peers into an MSDP mesh group so as to avoid flooding of SA messages between MSDP peers.

An MSDP mesh group refers to a group of MSDP peers that have MSDP peering relationship among one another and share the same group name.

4. SA messages are forwarded from one MSDP peer to another, and finally the information about the multicast source traverses all PIM-SM domains with MSDP peers (PIM-SM 2 and PIM-SM 3, in this example).
5. After receiving the SA message that RP 1 created, RP 2 in PIM-SM 2 determines whether any receivers for the multicast group exist in the domain.
 - If receivers for the multicast group exist in the domain, the RPT for the multicast group G is maintained between RP 2 and the receivers. RP 2 creates an (S, G) entry and sends an (S, G) join message hop by hop toward DR 1 at the multicast source side, so that it can directly join the SPT rooted at the source over other PIM-SM domains. Then, the multicast data can flow along the SPT to RP 2 and RP 2 can forward the data to the receivers along the RPT. After receiving the multicast traffic, the DR at the receiver side (DR 2) determines whether to initiate an RPT-to-SPT switchover process.
 - If no receivers for the group exist in the domain, RP 2 neither creates an (S, G) entry nor joins the SPT rooted at the source.

NOTE:

When using MSDP for inter-domain multicasting, once an RP receives information from a multicast source, it no longer relies on RPs in other PIM-SM domains. The receivers can override the RPs in other domains and directly join the multicast source-based SPT.

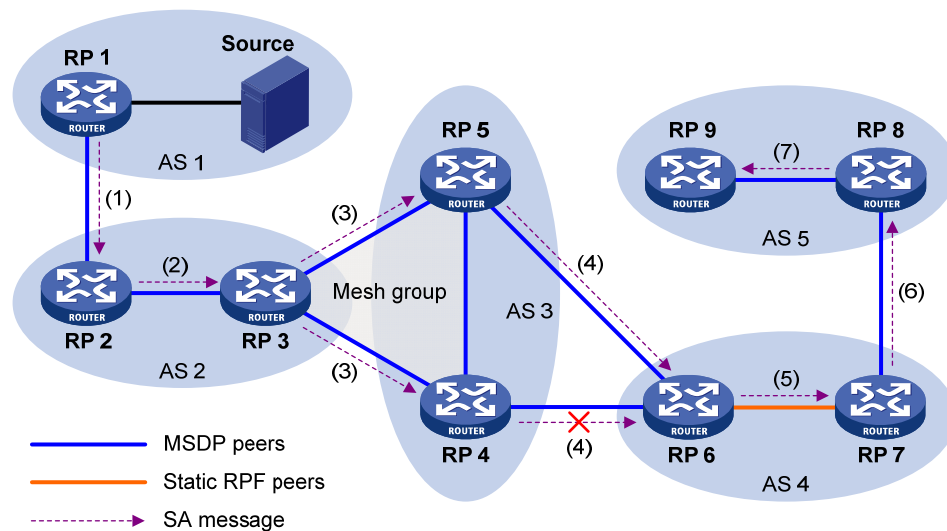
RPF check rules for SA messages

As shown in [Figure 60](#), the autonomous systems in the network are AS 1 through AS 5, with IGP enabled on routers within each AS and BGP or MBGP as the interoperation protocol among different ASs. Each AS contains at least one PIM-SM domain, and each PIM-SM domain contains one or more RPs. MSDP peering relationship has been established among different RPs. RP 3, RP 4, and RP 5 are in an MSDP mesh group. On RP 7, RP 6 is configured as its static RPF peer.

NOTE:

When an RP receives an SA message from a static RPF peer, the RP accepts the SA message and forwards it to other peers without performing an RPF check.

Figure 60 Diagram for RPF check for SA messages



As shown in Figure 60, these MSDP peers dispose of SA messages according to the following RPF check rules:

1. When RP 2 receives an SA message from RP 1:

Because the source-side RP address carried in the SA message is the same as the MSDP peer address, which means that the MSDP peer where the SA is from is the RP that has created the SA message, RP 2 accepts the SA message and forwards it to its other MSDP peer (RP 3).
2. When RP 3 receives the SA message from RP 2:

Because the SA message is from an MSDP peer (RP 2) in the same AS, and the MSDP peer is the next hop on the optimal path to the source-side RP, RP 3 accepts the message and forwards it to other peers (RP 4 and RP 5).
3. When RP 4 and RP 5 receive the SA message from RP 3:

Because the SA message is from an MSDP peer (RP 3) in the same mesh group, RP 4 and RP 5 both accept the SA message, but they do not forward the message to other members in the mesh group. Instead, they forward it to other MSDP peers (RP 6 in this example) out of the mesh group.
4. When RP 6 receives the SA messages from RP 4 and RP 5 (supposing RP 5 has a higher IP address):

Although RP 4 and RP 5 are in the same AS (AS 3) and both are MSDP peers of RP 6, because RP 5 has a higher IP address, RP 6 accepts only the SA message from RP 5.
5. When RP 7 receives the SA message from RP 6:

Because the SA message is from a static RPF peer (RP 6), RP 7 accepts the SA message and forwards it to other peer (RP 8).
6. When RP 8 receives the SA message from RP 7:

A BGP or MBGP route exists between two MSDP peers in different ASs. Because the SA message is from an MSDP peer (RP 7) in a different AS, and the MSDP peer is the next hop on the BGP or

MBGP route to the source-side RP, RP 8 accepts the message and forwards it to its other peer (RP 9).

7. When RP 9 receives the SA message from RP 8:

Because RP 9 has only one MSDP peer, RP 9 accepts the SA message.

SA messages from paths other than those described previously are not accepted or forwarded by MSDP peers.

Intra-domain Anycast RP through MSDP

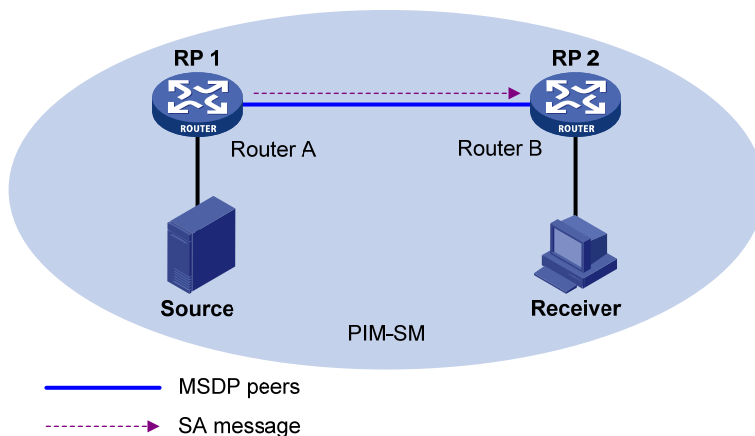
Anycast RP refers to an application that enables load balancing and redundancy backup between two or more RPs within a PIM-SM domain by configuring the same IP address for, and establishing MSDP peering relationship between, these RPs.

Usually an Anycast RP address is configured on a logic interface, like a loopback interface. An MSDP peer address must be different from the Anycast RP address.

Be sure to configure a 32-bit subnet mask (255.255.255.255) for the Anycast RP address sure, which means configure the Anycast RP address into a host address.

As shown in Figure 61, within a PIM-SM domain, a multicast source sends multicast data to multicast group G, and Receiver is a member of the multicast group. To implement Anycast RP, configure the same IP address (known as Anycast RP address, typically a private address) on Router A and Router B, configure these interfaces as C-RPs, and establish an MSDP peering relationship between Router A and Router B.

Figure 61 Intra-domain Anycast RP through MSDP



The work process of Anycast RP is as follows:

1. The multicast source registers with the nearest RP. In this example, Source registers with RP 1, with its multicast data encapsulated in the register message. When the register message arrives at RP 1, RP 1 de-encapsulates the message.
2. Receivers send join messages to the nearest RP to join in the RPT rooted as this RP. In this example, Receiver joins the RPT rooted at RP 2.

3. RPs share the registered multicast information by means of SA messages. In this example, RP 1 creates an SA message and sends it to RP 2, with the multicast data from Source encapsulated in the SA message. When the SA message reaches RP 2, RP 2 de-encapsulates the message.
4. Receivers receive the multicast data along the RPT and directly join the SPT rooted at the multicast source. In this example, RP 2 forwards the multicast data down the RPT. When Receiver receives the multicast data from Source, it directly joins the SPT rooted at Source.

The significance of Anycast RP is as follows:

- **Optimal RP path**—A multicast source registers with the nearest RP so that an SPT with the optimal path is built. A receiver joins the nearest RP so that an RPT with the optimal path is built.
- **Load balancing between RPs**—Each RP maintains just part of the source/group information within the PIM-SM domain and forward part of the multicast data, thereby achieving load balancing between different RPs.
- **Redundancy backup between RPs**—When an RP fails, the multicast source that previously registered with the RP or the receivers that previously joined the RP will register with or join another nearest RP, thereby achieving redundancy backup between RPs.

MSDP support for VPNs

The interfaces on the multicast routers in a VPN can set up MSDP peering relationship between each other. By exchanging SA messages between MSDP peers, multicast transmission in a VPN between different PIM-SM domains can be implemented.

To support MSDP for VPNs, a multicast router that runs MSDP maintains an independent set of MSDP mechanism for each VPN that it supports, including SA cache, peering connection, timers, sending cache, and cache for exchanging PIM messages. The information in one VPN is isolated from another, and MSDP and PIM-SM messages can be exchanged only within the same VPN.

Protocols and standards

- RFC 3618, *Multicast Source Discovery Protocol (MSDP)*
- RFC 3446, *Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*

MSDP configuration task list

Task	Remarks	
Configuring basic MSDP functions	Enabling MSDP	Required
	Creating an MSDP peer connection	Required
	Configuring a static RPF peer	Optional
Configuring an MSDP peer	Configuring MSDP peer description	Optional

Task		Remarks
connection	Configuring an MSDP mesh group	Optional
	Configuring MSDP peer connection control	Optional
Configuring SA messages related parameters	Configuring SA message content	Optional
	Configuring SA request messages	Optional
	Configuring SA message filtering rules	Optional
	Configuring the SA cache mechanism	Optional

Configuring basic MSDP functions

All the configuration tasks should be carried out on RPs in PIM-SM domains, and each of these RPs acts as an MSDP peer.

Configuration prerequisites

Before you configure basic MSDP functions, complete the following tasks:

- Configure any unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Configure PIM-SM to enable intra-domain multicast forwarding.
- Determine the IP addresses of MSDP peers.
- Determine the address prefix list for an RP address filtering policy.

Enabling MSDP

To enable MSDP globally for the public network:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IP multicast routing.	multicast routing-enable	Disabled by default.
3. Enable MSDP and enter public network MSDP view.	msdp	Disabled by default.

To enable MSDP in a VPN instance:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a VPN instance and enter VPN instance view.	ip vpn-instance <i>vpn-instance-name</i>	N/A

Step	Command	Remarks
3. Configure a route-distinguisher (RD) for the VPN instance.	route-distinguisher <i>route-distinguisher</i>	No RD is configured by default.
4. Enable IP multicast routing.	multicast routing-enable	Disabled by default.
5. Return to system view.	quit	N/A
6. Enable MSDP and enter VPN instance MSDP view.	msdp vpn-instance <i>vpn-instance-name</i>	Disabled by default.

For more information about the **ip vpn-instance** and **route-distinguisher** commands, see *IP Routing Command Reference*.

For more information about the **multicast routing-enable** command, see *IP Multicast Command Reference*.

Creating an MSDP peer connection

An MSDP peering relationship is identified by an address pair, namely, the address of the local MSDP peer and that of the remote MSDP peer. An MSDP peer connection must be created on both devices that are a pair of MSDP peers.

To create an MSDP peer connection:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network MSDP view or VPN instance MSDP view.	msdp [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Create an MSDP peer connection.	peer peer-address connect-interface <i>interface-type interface-number</i>	No MSDP peer connection is created by default.

NOTE:

If an interface of the router is shared by an MSDP peer and a BGP or MBGP peer at the same time, HP recommends you to configure the IP address of the MSDP peer the same as that of the BGP or MBGP peer.

Configuring a static RPF peer

Configuring static RPF peers avoids RPF check of SA messages.

To configure a static RPF peer:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network MSDP view or VPN instance MSDP view.	msdp [vpn-instance <i>vpn-instance-name</i>]	N/A

Step	Command	Remarks
3. Configure a static RPF peer.	static-rpf-peer <i>peer-address</i> [rp-policy <i>ip-prefix-name</i>]	No static RPF peer is configured by default.

NOTE:

If only one MSDP peer is configured on a router, this MSDP will be registered as a static RPF peer.

Configuring an MSDP peer connection

Before you configure an MSDP peer connection, complete the following tasks:

- Configure any unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Configure basic MSDP functions.
- Determine the description of MSDP peers.
- Determine the name of an MSDP mesh group.
- Determine the MSDP peer connection retry interval.
- Determine the MD5 authentication password for the TCP connection to be established with an MSDP peer.

Configuring MSDP peer description

With the MSDP peer description information, the administrator can easily distinguish different MSDP peers to better manage MSDP peers.

To configure description for an MSDP peer:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network MSDP view or VPN instance MSDP view.	msdp [vpn-instance <i>vpn-instance-name</i>]	N/A
3. Configure description for an MSDP peer.	peer <i>peer-address</i> description <i>text</i>	No description is configured for an MSDP peer by default.

Configuring an MSDP mesh group

An AS can contain multiple MSDP peers. You can use the MSDP mesh group mechanism to avoid SA message flooding among these MSDP peers and optimize the multicast traffic.

An MSDP peer in an MSDP mesh group forwards SA messages (that have passed the RPF check) from outside the mesh group to the other members in the mesh group. A mesh group member accepts SA messages from inside the group without performing an RPF check, and does not forward the message

within the mesh group. This mechanism not only avoids SA flooding but also simplifies the RPF check mechanism because you do not need to run BGP or MBGP between these MSDP peers.

By configuring the same mesh group name for multiple MSDP peers, you can create a mesh group that contains these MSDP peers.

! **IMPORTANT:**

Before grouping multiple routers into an MSDP mesh group, make sure that these routers are interconnected with one another.

To create an MSDP mesh group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network MSDP view or VPN instance MSDP view.	msdp [vpn-instance vpn-instance-name]	N/A
3. Create an MSDP mesh group and assign an MSDP peer to that mesh group.	peer peer-address mesh-group name	An MSDP peer does not belong to any mesh group by default. If you assign an MSDP peer to multiple mesh groups, only the last configuration is effective.

Configuring MSDP peer connection control

MSDP peers are interconnected over TCP (port number 639). You can flexibly control sessions between MSDP peers by manually deactivating and reactivating the MSDP peering connections. When the connection between two MSDP peers is deactivated, SA messages will no longer be delivered between them, and the TCP connection is closed without any connection setup retry. The configuration information, however, remain unchanged.

A TCP connection is required in the following situations:

- When a new MSDP peer is created
- When you reactivate a previously deactivated MSDP peer connection
- When a previously failed MSDP peer attempts to resume operation

You can adjust the interval between MSDP peering connection retries.

To enhance MSDP security, you can configure an MD5 authentication password for the TCP connection to be established with an MSDP peer. If the MD5 authentication fails, the TCP connection cannot be established.

! **IMPORTANT:**

The MSDP peers involved in the MD5 authentication must have the same authentication method and password. Otherwise, the authentication fails and the TCP connection cannot be established.

To configure MSDP peer connection control:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network MSDP view or VPN instance MSDP view.	msdp [vpn-instance vpn-instance-name]	N/A
3. Deactivate an MSDP peer.	shutdown peer-address	Optional. Active by default.
4. Configure the interval between MSDP peer connection retries.	timer retry interval	Optional. 30 seconds by default.
5. Configure an MD5 authentication key for the TCP connection to be established with an MSDP peer.	peer peer-address password { cipher simple } password	Optional. By default, MD5 authentication is not performed before a TCP connection is established.

Configuring SA messages related parameters

Before you configure SA message delivery, complete the following tasks:

- Configure any unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Configure basic MSDP functions.
- Determine the ACL rules for filtering SA request messages.
- Determine the ACL rules as SA message creation rules.
- Determine the ACL rules for filtering SA messages to be received and forwarded.
- Determine the TTL threshold for multicast packet encapsulation in SA messages.
- Determine the maximum number of (S, G) entries learned from the specified MSDP peer that the router can cache.

Configuring SA message content

Some multicast sources send multicast data at an interval longer than the aging time of (S, G) entries. In this case, the source-side DR must encapsulate multicast data packet by packet in register messages and send them to the source-side RP. The source-side RP transmits the (S, G) information to the remote RP through SA messages. Then the remote RP joins the source-side DR and builds an SPT. Because the (S, G) entries have timed out, remote receivers can never receive the multicast data from the multicast source.

After the source-side RP is enabled to encapsulate multicast data in SA messages, if the RP wants to send a multicast packet, it encapsulates the multicast packet in an SA message and sends it. After receiving the SA message, the remote RP de-encapsulates the SA message and delivers the multicast packet to the receivers in the local domain along the RPT.

The MSDP peers deliver SA messages to one another. After receiving an SA message, a router performs RPF check on the message. If the router finds that the remote RP address is the same as the local RP address, it discards the SA message. In the Anycast RP application, however, you must configure RPs with the same IP address on two or more routers in the same PIM-SM domain and configure these routers as MSDP peers to one another. Therefore, a logic RP address (namely, the RP address on the logic interface) that is different from the actual RP address must be designated for SA messages so that the messages can pass the RPF check.

To configure the SA message content:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network MSDP view or VPN instance MSDP view.	msdp [vpn-instance vpn-instance-name]	N/A
3. Enable encapsulation of multicast data in SA messages.	encap-data-enable	Optional. Disabled by default.
4. Configure the interface address as the RP address in SA messages.	originating-rp interface-type interface-number	Optional. PIM RP address by default.

Configuring SA request messages

By default, after receiving a new join message, a router does not send an SA request message to any MSDP peer. Instead, it waits for the next SA message from its MSDP peer. This will cause the receiver to delay obtaining multicast source information. To enable a new receiver to get the active multicast source information as early as possible, you can configure routers to send SA request messages to the designated MSDP peers after receiving a join message of a new receiver.

! IMPORTANT:

Before you can enable the device to send SA requests, be sure to disable the SA message cache mechanism.

To configure SA message transmission and filtering:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network MSDP view or VPN instance MSDP view.	msdp [vpn-instance vpn-instance-name]	N/A
3. Enable the device to send SA request messages.	peer peer-address request-sa-enable	Optional. Disabled by default.
4. Configure a filtering rule for SA request messages.	peer peer-address sa-request-policy [acl acl-number]	Optional. SA request messages are not filtered by default.

Configuring SA message filtering rules

By configuring an SA message creation rule, you can enable the router to filter the (S, G) entries to be advertised when creating an SA message, so that the propagation of messages of multicast sources is controlled.

By configuring a filtering rule for receiving or forwarding SA messages, you can enable the router to filter the (S, G) forwarding entries to be advertised when receiving or forwarding an SA message, so that the propagation of multicast source information is controlled at SA message reception or forwarding.

By configuring a TTL threshold for multicast data packet encapsulation in SA messages, you can control the multicast data packet encapsulation in SA messages and limit the propagation range of SA messages:

- Before creating an SA message with an encapsulated multicast data packet, the router checks the TTL value of the multicast data packet. If the TTL value is less than the threshold, the router does not create an SA message. If the TTL value is greater than or equal to the threshold, the router encapsulates the multicast data in an SA message and sends the SA message.
- After receiving an SA message with an encapsulated multicast data packet, the router decreases the TTL value of the multicast packet by 1 and then checks the TTL value. If the TTL value is less than the threshold, the router does not forward the SA message to the designated MSDP peer. If the TTL value is greater than or equal to the threshold, the router re-encapsulates the multicast data in an SA message and sends the SA message.

To configure a filtering rule for receiving or forwarding SA messages:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network MSDP view or VPN instance MSDP view.	msdp [vpn-instance vpn-instance-name]	N/A
3. Configure an SA message creation rule.	import-source [acl acl-number]	No restrictions on (S, G) entries by default.
4. Configure a filtering rule for receiving or forwarding SA messages.	peer peer-address sa-policy { import export } [acl acl-number]	No filtering rule by default.
5. Configure the TTL threshold for multicast data packet encapsulation in SA messages.	peer peer-address minimum-ttl ttl-value	Optional. 0 by default.

Configuring the SA cache mechanism

To reduce the time spent in obtaining the multicast information, you can enable the SA cache mechanism to cache (S, G) entries contained in SA messages locally on the router. However, caching (S, G) entries uses memory space on the router.

When the SA cache mechanism is enabled and the router receives a new (*, G) join message, the router searches its SA cache first.

- If the corresponding (S, G) entry does not exist in the cache, the router waits for the SA message that its MSDP peer will send in the next cycle.
- If the corresponding (S, G) entry exists in the cache, the router joins the corresponding SPT rooted at S.

To protect the router effectively against denial of service (DoS) attacks, you can set a limit on the number of (S, G) entries the router can cache.

To configure the SA message cache:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter public network MSDP view or VPN instance MSDP view.	msdp [vpn-instance vpn-instance-name]	N/A
3. Enable the SA cache mechanism.	cache-sa-enable	Optional. Enabled by default.
4. Configure the maximum number of (S, G) entries learned from the specified MSDP peer that the router can cache.	peer peer-address sa-cache-maximum sa-limit	Optional. 8192 by default.

Displaying and maintaining MSDP

Step	Command	Remarks
1. Display brief information about MSDP peers.	display msdp [all-instance vpn-instance vpn-instance-name] brief [state { connect down listen shutdown up }] [{ begin exclude include } regular-expression]	Available in any view
2. Display detailed information about the status of MSDP peers.	display msdp [all-instance vpn-instance vpn-instance-name] peer-status [peer-address] [{ begin exclude include } regular-expression]	Available in any view
3. Display the (S, G) entry information in the SA cache.	display msdp [all-instance vpn-instance vpn-instance-name] sa-cache [group-address source-address as-number] * [{ begin exclude include } regular-expression]	Available in any view
4. Display the number of (S, G) entries in the SA cache.	display msdp [all-instance vpn-instance vpn-instance-name] sa-count [as-number] [{ begin exclude include } regular-expression]	Available in any view

Step	Command	Remarks
5. Reset the TCP connection with an MSDP peer.	reset msdp [all-instance vpn-instance <i>vpn-instance-name</i>] peer [<i>peer-address</i>]	Available in user view
6. Clear (S, G) entries in the SA cache.	reset msdp [all-instance vpn-instance <i>vpn-instance-name</i>] sa-cache [<i>group-address</i>]	Available in user view
7. Clear statistics for an MSDP peer.	reset msdp [all-instance vpn-instance <i>vpn-instance-name</i>] statistics [<i>peer-address</i>]	Available in user view

MSDP configuration examples

PIM-SM Inter-domain multicast configuration

Network requirements

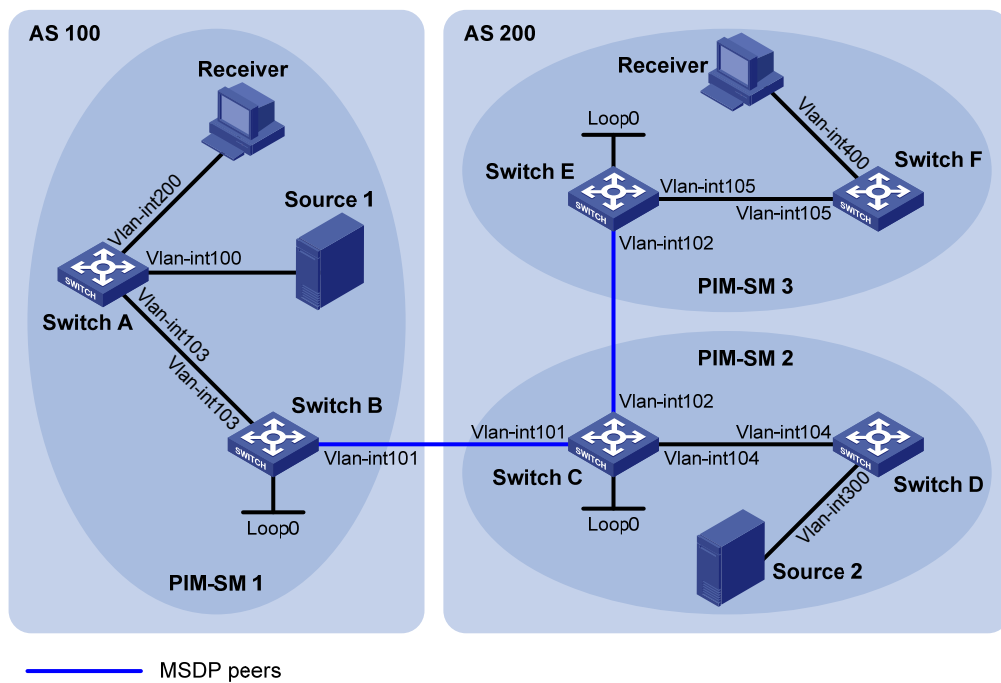
As shown in [Figure 62](#), AS 100 and AS 200 run OSPF within each AS, and run BGP between each other.

PIM-SM 1 belongs to AS 100, and PIM-SM 2 and PIM-SM 3 belong to AS 200. Each PIM-SM domain has at least one multicast source or receiver.

Loopback 0 is configured as the C-BSR and C-RP of the related PIM-SM domain on Switch B, Switch C, and Switch E, respectively.

An MSDP peering relationship is set up between the RPs of the PIM-SM domains to share multicast source information among the PIM-SM domains.

Figure 62 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int103	10.110.1.2/24	Switch D	Vlan-int104	10.110.4.2/24
	Vlan-int100	10.110.2.1/24		Vlan-int300	10.110.5.1/24
	Vlan-int200	10.110.3.1/24	Switch E	Vlan-int105	10.110.6.1/24
Switch B	Vlan-int103	10.110.1.1/24		Vlan-int102	192.168.3.2/24
	Vlan-int101	192.168.1.1/24		Loop0	3.3.3.3/32
	Loop0	1.1.1.1/32	Switch F	Vlan-int105	10.110.6.2/24
Switch C	Vlan-int104	10.110.4.1/24		Vlan-int400	10.110.7.1/24
	Vlan-int102	192.168.3.1/24	Source 1	—	10.110.2.100/24
	Vlan-int101	192.168.1.2/24	Source 2	—	10.110.5.100/24
	Loop0	2.2.2.2/32			

Configuration procedure

1. Configure the IP address and subnet mask for each interface as per Figure 62. (Details not shown.)
2. Configure OSPF on switches in each AS to make sure the switches in each AS are interoperable at the network-layer, and they can dynamically update their routing information. (Details not shown.)
3. Enable IP multicast routing, enable PIM-SM on each interface, and configure a PIM-SM domain border:

Enable IP multicast routing on Switch A, enable PIM-SM on each interface, and enable IGMP on the host-side interface VLAN-interface 200.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim sm
```

```
[SwitchA-Vlan-interface103] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] igmp enable
[SwitchA-Vlan-interface200] pim sm
[SwitchA-Vlan-interface200] quit
```

Enable IP multicast routing, enable PIM-SM on each interface, and enable IGMP on Switch B, Switch C, Switch D, Switch E, and Switch F in the same way. (Details not shown.)

Configure a PIM domain border on Switch B.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim bsr-boundary
[SwitchB-Vlan-interface101] quit
```

Configure a PIM domain border on Switch C and Switch E in the same way. (Details not shown.)

4. Configure C-BSRs and C-RPs:

Configure Loopback 0 as a C-BSR and a C-RP on Switch B.

```
[SwitchB] pim
[SwitchB-pim] c-bsr loopback 0
[SwitchB-pim] c-rp loopback 0
[SwitchB-pim] quit
```

Configure C-BSRs and C-RPs on Switch C and Switch E in the same way. (Details not shown.)

5. Configure BGP for mutual route redistribution between BGP and OSPF:

Configure an EBGP peer, and redistribute OSPF routes on Switch B.

```
[SwitchB] bgp 100
[SwitchB-bgp] router-id 1.1.1.1
[SwitchB-bgp] peer 192.168.1.2 as-number 200
[SwitchB-bgp] import-route ospf 1
[SwitchB-bgp] quit
```

Configure an EBGP peer, and redistribute OSPF routes on Switch C.

```
[SwitchC] bgp 200
[SwitchC-bgp] router-id 2.2.2.2
[SwitchC-bgp] peer 192.168.1.1 as-number 100
[SwitchC-bgp] import-route ospf 1
[SwitchC-bgp] quit
```

Redistribute BGP routes into OSPF on Switch B.

```
[SwitchB] ospf 1
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] quit
```

Redistribute BGP routes into OSPF on Switch C.

```
[SwitchB] ospf 1
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] quit
```

6. Configure MSDP peers:

Configure an MSDP peer on Switch B.

```
[SwitchB] msdp
[SwitchB-msdp] peer 192.168.1.2 connect-interface vlan-interface 101
[SwitchB-msdp] quit
```

Configure an MSDP peer on Switch C.

```
[SwitchC] msdp
[SwitchC-msdp] peer 192.168.1.1 connect-interface vlan-interface 101
[SwitchC-msdp] peer 192.168.3.2 connect-interface vlan-interface 102
[SwitchC-msdp] quit
```

Configure MSDP peers on Switch E.

```
[SwitchE] msdp
[SwitchE-msdp] peer 192.168.3.1 connect-interface vlan-interface 102
[SwitchE-msdp] quit
```

Verifying the configuration

Use the **display bgp peer** command to display the BGP peering relationship between the switches. For example:

Display information about BGP peering relationship on Switch B.

```
[SwitchB] display bgp peer

BGP local router ID : 1.1.1.1
Local AS number : 100
Total number of peers : 1                Peers in established state : 1

Peer                AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
-----
192.168.1.2         200    24      21      0      6 00:13:09 Established
```

Display information about BGP peering relationship on Switch C.

```
[SwitchC] display bgp peer

BGP local router ID : 2.2.2.2
Local AS number : 200
Total number of peers : 1                Peers in established state : 1

Peer                AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
-----
192.168.1.1         100    18      16      0      1 00:12:04 Established
```

To display BGP routing table information on the switches, use the **display bgp routing-table** command. For example:

Display BGP routing table information on Switch C.

```
[SwitchC] display bgp routing-table

Total Number of Routes: 5

BGP Local router ID is 2.2.2.2
```

Status codes: * - valid, ^ - VPNv4 best, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* > 1.1.1.1/32	192.168.1.1	0		0	100?
* >i 2.2.2.2/32	0.0.0.0	0		0	?
* > 192.168.1.0	0.0.0.0	0		0	?
* > 192.168.1.1/32	0.0.0.0	0		0	?
* > 192.168.1.2/32	0.0.0.0	0		0	?

When the multicast source in PIM-SM 1 (Source 1) and the multicast source in PIM-SM 2 (Source 2) send multicast information, receivers in PIM-SM 1 and PIM-SM 3 can receive the multicast data. You can use the **display msdp brief** command to display the brief information of MSDP peering relationship between the switches. For example:

Display brief information about MSDP peering relationship on Switch B.

```
[SwitchB] display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
```

Configured	Up	Listen	Connect	Shutdown	Down
1	1	0	0	0	0

Peer's Address	State	Up/Down time	AS	SA Count	Reset Count
192.168.1.2	Up	00:12:27	200	13	0

Display brief information about MSDP peering relationship on Switch C.

```
[SwitchC] display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
```

Configured	Up	Listen	Connect	Shutdown	Down
2	2	0	0	0	0

Peer's Address	State	Up/Down time	AS	SA Count	Reset Count
192.168.3.2	Up	00:15:32	200	8	0
192.168.1.1	Up	00:06:39	100	13	0

Display brief information about MSDP peering relationship on Switch E.

```
[SwitchE] display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
```

Configured	Up	Listen	Connect	Shutdown	Down
1	1	0	0	0	0

Peer's Address	State	Up/Down time	AS	SA Count	Reset Count
192.168.3.1	Up	01:07:08	200	8	0

Display detailed MSDP peer information on Switch B.

```
[SwitchB] display msdp peer-status
MSDP Peer Information of VPN-Instance: public net
MSDP Peer 192.168.1.2, AS 200
Description:
```

```
Information about connection status:
  State: Up
  Up/down time: 00:15:47
  Resets: 0
  Connection interface: Vlan-interface101 (192.168.1.1)
  Number of sent/received messages: 16/16
  Number of discarded output messages: 0
  Elapsed time since last connection or counters clear: 00:17:51
Information about (Source, Group)-based SA filtering policy:
  Import policy: none
  Export policy: none
Information about SA-Requests:
  Policy to accept SA-Request messages: none
  Sending SA-Requests status: disable
Minimum TTL to forward SA with encapsulated data: 0
SAs learned from this peer: 0, SA-cache maximum for the peer: none
Input queue size: 0, Output queue size: 0
Counters for MSDP message:
  Count of RPF check failure: 0
  Incoming/outgoing SA messages: 0/0
  Incoming/outgoing SA requests: 0/0
  Incoming/outgoing SA responses: 0/0
  Incoming/outgoing data packets: 0/0
```

Inter-AS multicast configuration by leveraging static RPF peers

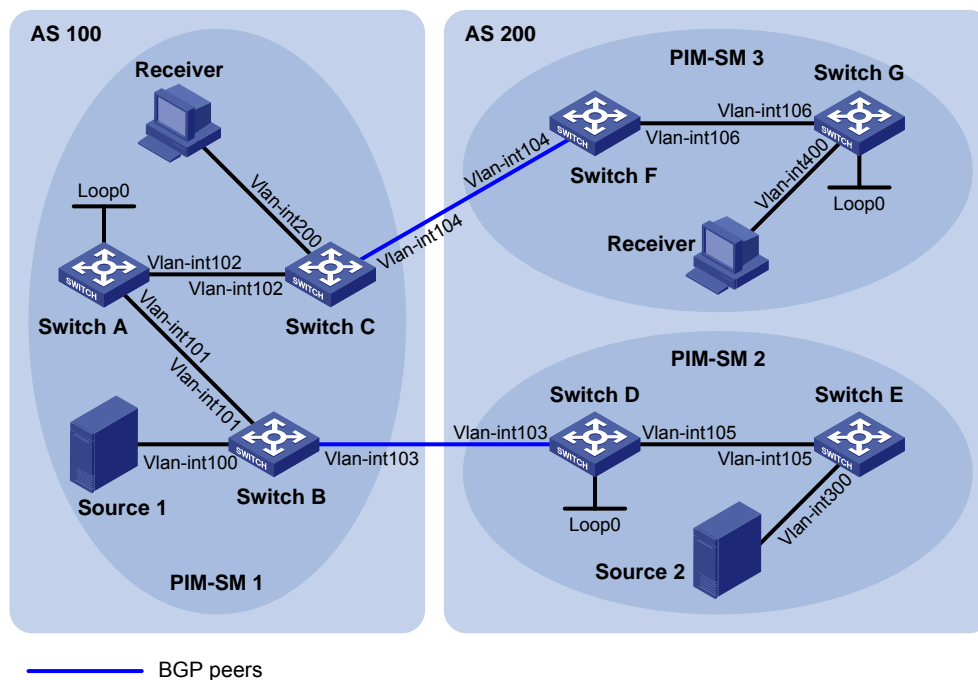
Network requirements

As shown in [Figure 63](#), AS 100 and AS 200 run OSPF within each AS, and run BGP between each other. PIM-SM 1 belongs to AS 100, and PIM-SM 2 and PIM-SM 3 belong to AS 200. Each PIM-SM domain has at least one multicast source or receiver.

Loopback 0 is configured as a C-BSR and a C-RP of the related PIM-SM domain on Switch A, Switch D, and Switch G, respectively.

According to the RPF principle, the device can receive SA messages that pass the filtering policy from its static RPF peers. To share multicast source information among PIM-SM domains without changing the unicast topology structure, configure MSDP peering relationship for the RPs of the PIM-SM domains and configure static RPF peering relationship for the MSDP peers to share multicast source information among the PIM-SM domains.

Figure 63 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Source 1	-	192.168.1.100/24	Switch D	Vlan-int105	10.110.5.1/24
Source 2	-	192.168.3.100/24		Vlan-int103	10.110.3.2/24
Switch A	Vlan-int101	10.110.1.1/24		Loop0	2.2.2.2/32
	Vlan-int102	10.110.2.1/24	Switch E	Vlan-int105	10.110.5.2/24
	Loop0	1.1.1.1/32		Vlan-int300	192.168.3.1/24
Switch B	Vlan-int101	10.110.1.2/24	Switch F	Vlan-int106	10.110.6.1/24
	Vlan-int100	192.168.1.1/24		Vlan-int104	10.110.4.2/24
	Vlan-int103	10.110.3.1/24	Switch G	Vlan-int106	10.110.6.2/24
Switch C	Vlan-int102	10.110.2.2/24		Vlan-int400	192.168.4.1/24
	Vlan-int200	192.168.2.1/24		Loop0	3.3.3.3/32
	Vlan-int104	10.110.4.1/24			

Configuration procedure

1. Configure the IP address and subnet mask for each interface as per Figure 63. (Details not shown.)
2. Configure OSPF on the switches in each AS to make sure the switches in each AS are interoperable at the network-layer, and they can dynamically update their routing information. (Details not shown.)
3. Enable IP multicast routing, enable PIM-SM and IGMP, and configure a PIM-SM domain border:
Enable IP multicast routing on Switch C, enable PIM-SM on each interface, and enable IGMP on the host-side interface VLAN-interface 200.

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 102
[SwitchC-Vlan-interface102] pim sm
```

```
[SwitchC-Vlan-interface102] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] igmp enable
[SwitchC-Vlan-interface200] pim sm
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 104
[SwitchC-Vlan-interface104] pim sm
[SwitchC-Vlan-interface104] quit
```

Enable IP multicast routing, PIM-SM and IGMP on Switch A, Switch B, Switch D, Switch E, Switch F, and Switch G in the same way. (Details not shown.)

Configure PIM domain borders on Switch B.

```
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] pim bsr-boundary
[SwitchB-Vlan-interface103] quit
```

Configure PIM domain borders on Switch C, Switch D, and Switch F in the same way. (Details not shown.)

4. Configure C-BSRs and C-RPs:

Configure Loopback 0 as a C-BSR and a C-RP on Switch A.

```
[SwitchA] pim
[SwitchA-pim] c-bsr loopback 0
[SwitchA-pim] c-rp loopback 0
[SwitchA-pim] quit
```

Configure C-BSRs and C-RPs on Switch D and Switch G in the same way. (Details not shown.)

5. Configure BGP, and redistribute BGP routing information into OSPF, and OSPF routing information into BGP:

Configure the EBGP peer, and redistribute OSPF routing information on Switch B.

```
[SwitchB] bgp 100
[SwitchB-bgp] router-id 1.1.1.2
[SwitchB-bgp] peer 10.110.3.2 as-number 200
[SwitchB-bgp] import-route ospf 1
[SwitchB-bgp] quit
```

Configure the EBGP peer, and redistribute OSPF routing information on Switch D.

```
[SwitchD] bgp 200
[SwitchD-bgp] router-id 2.2.2.2
[SwitchD-bgp] peer 10.110.3.1 as-number 100
[SwitchD-bgp] import-route ospf 1
[SwitchD-bgp] quit
```

Configure the EBGP peer, and redistribute OSPF routing information on Switch C.

```
[SwitchC] bgp 100
[SwitchC-bgp] router-id 1.1.1.3
[SwitchC-bgp] peer 10.110.4.2 as-number 200
[SwitchC-bgp] import-route ospf 1
[SwitchC-bgp] quit
```

Configure the EBGP peer, and redistribute OSPF routing information on Switch F.

```
[SwitchF] bgp 200
[SwitchF-bgp] router-id 3.3.3.1
[SwitchF-bgp] peer 10.110.4.1 as-number 100
[SwitchF-bgp] import-route ospf 1
[SwitchF-bgp] quit
```

Redistribute BGP routing information into OSPF on Switch B.

```
[SwitchB] ospf 1
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] quit
```

Redistribute BGP routing information into OSPF on Switch D.

```
[SwitchD] ospf 1
[SwitchD-ospf-1] import-route bgp
[SwitchD-ospf-1] quit
```

Redistribute BGP routing information into OSPF on Switch C.

```
[SwitchC] ospf 1
[SwitchC-ospf-1] import-route bgp
[SwitchC-ospf-1] quit
```

Redistribute BGP routing information into OSPF on Switch F.

```
[SwitchF] ospf 1
[SwitchF-ospf-1] import-route bgp
[SwitchF-ospf-1] quit
```

6. Configure MSDP peers and static RPF peers:

Configure Switch D and Switch G as the MSDP peers and static RPF peers of Switch A.

```
[SwitchA] ip ip-prefix list-dg permit 10.110.0.0 16 greater-equal 16 less-equal 32
[SwitchA] msdp
[SwitchA-msdp] peer 10.110.3.2 connect-interface vlan-interface 101
[SwitchA-msdp] peer 10.110.6.2 connect-interface vlan-interface 102
[SwitchA-msdp] static-rpf-peer 10.110.3.2 rp-policy list-dg
[SwitchA-msdp] static-rpf-peer 10.110.6.2 rp-policy list-dg
[SwitchA-msdp] quit
```

Configure Switch A as the MSDP peer and static RPF peer of Switch D.

```
[SwitchD] ip ip-prefix list-a permit 10.110.0.0 16 greater-equal 16 less-equal 32
[SwitchD] msdp
[SwitchD-msdp] peer 10.110.1.1 connect-interface vlan-interface 103
[SwitchD-msdp] static-rpf-peer 10.110.1.1 rp-policy list-a
[SwitchD-msdp] quit
```

Configure Switch A as the MSDP peer and static RPF peer of Switch G.

```
[SwitchG] ip ip-prefix list-a permit 10.110.0.0 16 greater-equal 16 less-equal 32
[SwitchG] msdp
[SwitchG-msdp] peer 10.110.2.1 connect-interface vlan-interface 106
[SwitchG-msdp] static-rpf-peer 10.110.2.1 rp-policy list-a
[SwitchG-msdp] quit
```


Verifying the configuration

Use the **display bgp peer** command to display the BGP peering relationship between the switches. If the command gives no output information on Switch A, it means that no BGP peering relationship has been established between Switch A and Switch D, or between Switch A and Switch G.

When the multicast source in PIM-SM 1 (Source 1) and the multicast source in PIM-SM 2 (Source 2) send multicast information, receivers in PIM-SM 1 and PIM-SM 3 can receive the multicast data. You can use the **display msdp brief** command to display the brief information of MSDP peering relationship between the switches. For example:

Display brief MSDP peer information on Switch A.

```
[SwitchA] display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
  Configured   Up           Listen       Connect      Shutdown     Down
  2            2           0            0            0            0

  Peer's Address   State   Up/Down time   AS   SA Count   Reset Count
  10.110.3.2      Up      01:07:08      ?   8          0
  10.110.6.2      Up      00:16:39      ?   13         0
```

Display brief MSDP peer information on Switch D.

```
[SwitchD] display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
  Configured   Up           Listen       Connect      Shutdown     Down
  1            1           0            0            0            0

  Peer's Address   State   Up/Down time   AS   SA Count   Reset Count
  10.110.1.1      Up      01:07:09      ?   8          0
```

Display brief MSDP peer information on Switch G.

```
[SwitchG] display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
  Configured   Up           Listen       Connect      Shutdown     Down
  1            1           0            0            0            0

  Peer's Address   State   Up/Down time   AS   SA Count   Reset Count
  10.110.2.1      Up      00:16:40      ?   13         0
```

Anycast RP configuration

Network requirements

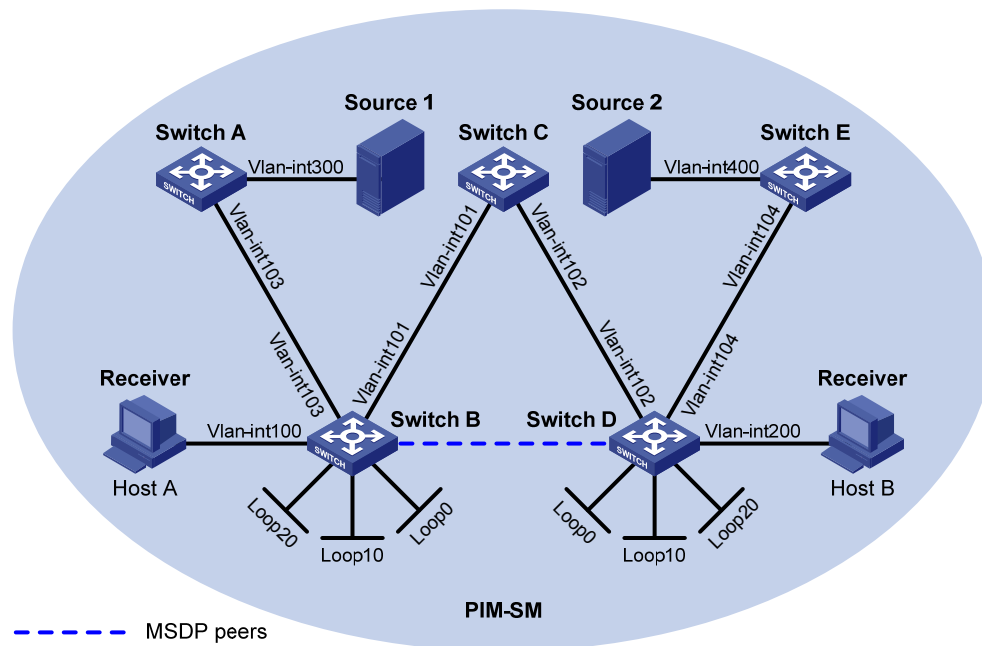
As shown in [Figure 64](#), the PIM-SM domain has multiple multicast sources and receivers. OSPF runs within the domain to provide unicast routes.

Configure the Anycast RP application so that the receiver-side DRs and the source-side DRs can initiate a join message to their respective RPs that are the topologically nearest to them.

On Switch B and Switch D, configure the interface Loopback 10 as a C-BSR, and Loopback 20 as a C-RP.

The router ID of Switch B is 1.1.1.1, and the router ID of Switch D is 2.2.2.2. Set up an MSDP peering relationship between Switch B and Switch D.

Figure 64 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Source 1	—	10.110.5.100/24	Switch C	Vlan-int101	192.168.1.2/24
Source 2	—	10.110.6.100/24		Vlan-int102	192.168.2.2/24
Switch A	Vlan-int300	10.110.5.1/24	Switch D	Vlan-int200	10.110.3.1/24
	Vlan-int103	10.110.2.2/24		Vlan-int104	10.110.4.1/24
Switch B	Vlan-int100	10.110.1.1/24		Vlan-int102	192.168.2.1/24
	Vlan-int103	10.110.2.1/24		Loop0	2.2.2.2/32
	Vlan-int101	192.168.1.1/24		Loop10	4.4.4.4/32
	Loop0	1.1.1.1/32		Loop20	10.1.1.1/32
	Loop10	3.3.3.3/32	Switch E	Vlan-int400	10.110.6.1/24
	Loop20	10.1.1.1/32		Vlan-int104	10.110.4.2/24

Configuration procedure

1. Configure the IP address and subnet mask for each interface as per Figure 64. (Details not shown.)
2. Configure OSPF on the switches to make sure the switches are interoperable at the network-layer, and they can dynamically update their routing information. (Details not shown.)
3. Enable IP multicast routing, IGMP and PIM-SM:

Enable IP multicast routing on Switch B, enable IGMP on the host-side interface VLAN-interface 100, and enable PIM-SM on each interface.

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp enable
```

```

[SwitchB-Vlan-interface100] pim sm
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] pim sm
[SwitchB-Vlan-interface103] quit
[SwitchB] interface Vlan-interface 101
[SwitchB-Vlan-interface101] pim sm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface loopback 0
[SwitchB-LoopBack0] pim sm
[SwitchB-LoopBack0] quit
[SwitchB] interface loopback 10
[SwitchB-LoopBack10] pim sm
[SwitchB-LoopBack10] quit
[SwitchB] interface loopback 20
[SwitchB-LoopBack20] pim sm
[SwitchB-LoopBack20] quit

```

Enable IP multicast routing, IGMP and PIM-SM on Switch A, Switch C, Switch D, and Switch E in the same way. (Details not shown.)

4. Configure C-BSRs and C-RPs:

Configure Loopback 10 as a C-BSR and Loopback 20 as a C-RP on Switch B.

```

[SwitchB] pim
[SwitchB-pim] c-bsr loopback 10
[SwitchB-pim] c-rp loopback 20
[SwitchB-pim] quit

```

Configure a C-BSRs and a C-RP on Switch D in the same way. (Details not shown.)

5. Configure MSDP peers:

Configure an MSDP peer on Loopback 0 of Switch B.

```

[SwitchB] msdp
[SwitchB-msdp] originating-rp loopback 0
[SwitchB-msdp] peer 2.2.2.2 connect-interface loopback 0
[SwitchB-msdp] quit

```

Configure an MSDP peer on Loopback 0 of Switch D.

```

[SwitchD] msdp
[SwitchD-msdp] originating-rp loopback 0
[SwitchD-msdp] peer 1.1.1.1 connect-interface loopback 0
[SwitchD-msdp] quit

```

Verifying the configuration

You can use the **display msdp brief** command to display the brief information of MSDP peering relationship between the switches.

Display brief MSDP peer information on Switch B.

```

[SwitchB] display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
  Configured   Up           Listen      Connect     Shutdown    Down

```

```

1          1          0          0          0          0

Peer's Address   State   Up/Down time   AS    SA Count   Reset Count
2.2.2.2         Up     00:10:17      ?     0          0

```

Display brief MSDP peer information on Switch D.

```

[SwitchD] display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
Configured   Up       Listen       Connect      Shutdown     Down
1            1        0            0            0            0

Peer's Address   State   Up/Down time   AS    SA Count   Reset Count
1.1.1.1         Up     00:10:18      ?     0          0

```

To display the PIM routing information on the switches, use the **display pim routing-table** command. When Source 1 10.110.5.100/24 sends multicast data to multicast group G 225.1.1.1, Host A joins multicast group G. By comparing the PIM routing information displayed on Switch B with that displayed on Switch D, you can see that Switch B acts now as the RP for Source 1 and Host A.

Display PIM routing information on Switch B.

```

[SwitchB] display pim routing-table
VPN-Instance: public net
Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)
  RP: 10.1.1.1 (local)
  Protocol: pim-sm, Flag: WC
  UpTime: 00:15:04
  Upstream interface: Register
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface100
      Protocol: igmp, UpTime: 00:15:04, Expires: -

(10.110.5.100, 225.1.1.1)
  RP: 10.1.1.1 (local)
  Protocol: pim-sm, Flag: SPT 2MSDP ACT
  UpTime: 00:46:28
  Upstream interface: Vlan-interface103
    Upstream neighbor: 10.110.2.2
    RPF prime neighbor: 10.110.2.2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface100
      Protocol: pim-sm, UpTime: - , Expires: -

```

Display PIM routing information on Switch D.

```

[SwitchD] display pim routing-table

```

No information is output on Switch D.

Host A has left multicast group G. Source 1 has stopped sending multicast data to multicast group G. When Source 2 10.110.6.100/24 sends multicast data to G, Host B joins G. By comparing the PIM routing information displayed on Switch B with that displayed on Switch D, you can see that Switch D acts now as the RP for Source 2 and Host B.

Display PIM routing information on Switch B.

```
[SwitchB] display pim routing-table
```

No information is output on Switch B.

Display PIM routing information on Switch D.

```
[SwitchD] display pim routing-table
```

```
VPN-Instance: public net
```

```
Total 1 (*, G) entry; 1 (S, G) entry
```

```
(*, 225.1.1.1)
```

```
RP: 10.1.1.1 (local)
```

```
Protocol: pim-sm, Flag: WC
```

```
UpTime: 00:12:07
```

```
Upstream interface: Register
```

```
Upstream neighbor: NULL
```

```
RPF prime neighbor: NULL
```

```
Downstream interface(s) information:
```

```
Total number of downstreams: 1
```

```
1: Vlan-interface200
```

```
Protocol: igmp, UpTime: 00:12:07, Expires: -
```

```
(10.110.6.100, 225.1.1.1)
```

```
RP: 10.1.1.1 (local)
```

```
Protocol: pim-sm, Flag: SPT 2MSDP ACT
```

```
UpTime: 00:40:22
```

```
Upstream interface: Vlan-interface104
```

```
Upstream neighbor: 10.110.4.2
```

```
RPF prime neighbor: 10.110.4.2
```

```
Downstream interface(s) information:
```

```
Total number of downstreams: 1
```

```
1: Vlan-interface200
```

```
Protocol: pim-sm, UpTime: - , Expires: -
```

SA message filtering configuration

Network requirements

As shown in [Figure 65](#), three PIM-SM domains exist in the network, and OSPF runs within and among the domains to provide unicast routing.

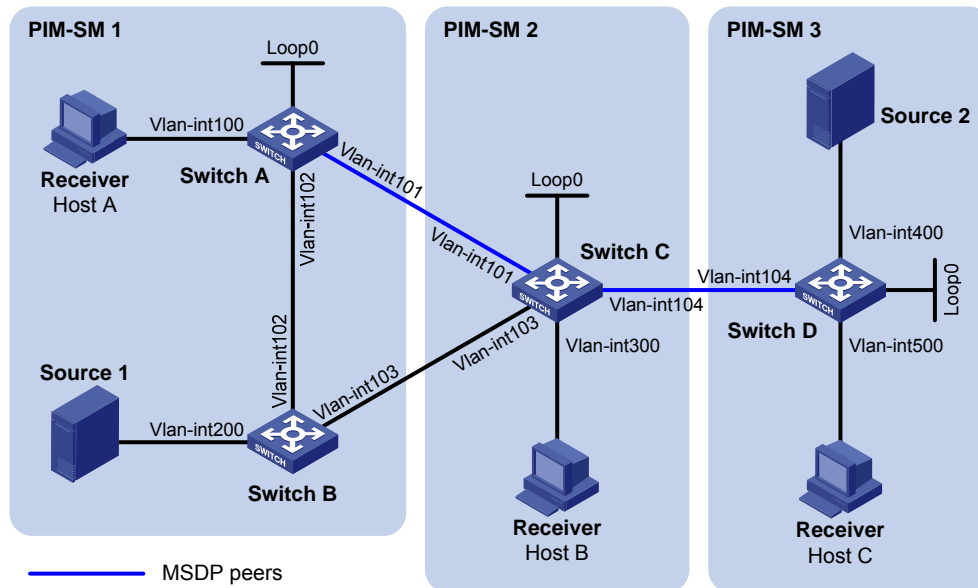
Loopback 0 is configured as a C-BSR and a C-RP in the related PIM-SM domains on Switch A, Switch C, and Switch D, respectively.

An MSDP peering relationship is set up between Switch A and Switch C and between Switch C and Switch D.

Source 1 sends multicast data to multicast groups 225.1.1.0/30 and 226.1.1.0/30, and Source 2 sends multicast data to multicast group 227.1.1.0/30.

Configure SA message filtering rules so that receivers Host A and Host B can receive only the multicast data addressed to multicast groups 225.1.1.0/30 and 226.1.1.0/30, and Host C can receive only the multicast data addressed to multicast groups 226.1.1.0/30 and 227.1.1.0/30.

Figure 65 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Source 1	—	10.110.3.100/24	Switch C	Vlan-int300	10.110.4.1/24
Source 2	—	10.110.6.100/24	Switch D	Vlan-int104	10.110.5.1/24
Switch A	Vlan-int100	10.110.1.1/24	Switch C	Vlan-int101	192.168.1.2/24
	Vlan-int102	10.110.2.1/24		Vlan-int103	192.168.2.2/24
	Vlan-int101	192.168.1.1/24		Loop0	2.2.2.2/32
	Loop0	1.1.1.1/32	Switch D	Vlan-int400	10.110.6.1/24
Switch B	Vlan-int200	10.110.3.1/24	Switch D	Vlan-int500	10.110.7.1/24
	Vlan-int102	10.110.2.2/24	Switch D	Vlan-int104	10.110.5.2/24
	Vlan-int103	192.168.2.1/24	Loop0	Loop0	3.3.3.3/32

Configuration Procedure

1. Configure the IP address and subnet mask for each interface as per Figure 65. (Details not shown.)
2. Configure OSPF on the switches to make sure the switches are interoperable at the network-layer, and they can dynamically update their routing information. (Details not shown.)
3. Enable IP multicast routing, IGMP and PIM-SM, and configure a PIM domain border:
 # On Switch A, enable IP multicast routing, enable IGMP on the host-side interface, VLAN-interface 100, and enable PIM-SM on each interface.

```

<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim sm
[SwitchA-Vlan-interface102] quit
[SwitchA] interface loopback 0
[SwitchA-LoopBack0] pim sm
[SwitchA-LoopBack0] quit

```

Enable IP multicast routing, IGMP and PIM-SM on Switch B, Switch C and Switch D in the same way. (Details not shown.)

Configure a PIM domain border on Switch C.

```

[SwitchC] interface vlan-interface 101
[SwitchC-Vlan-interface101] pim bsr-boundary
[SwitchC-Vlan-interface101] quit
[SwitchC] interface vlan-interface 103
[SwitchC-Vlan-interface103] pim bsr-boundary
[SwitchC-Vlan-interface103] quit
[SwitchC] interface vlan-interface 104
[SwitchC-Vlan-interface104] pim bsr-boundary
[SwitchC-Vlan-interface104] quit

```

Configure a PIM domain border on Switch A, Switch B and Switch D in the same way. (Details not shown.)

4. Configure C-BSRs and C-RPs:

Configure Loopback 0 as a C-BSR and a C-RP on Switch A.

```

[SwitchA] pim
[SwitchA-pim] c-bsr loopback 0
[SwitchA-pim] c-rp loopback 0
[SwitchA-pim] quit

```

Configure C-BSRs and C-RPs on Switch C and Switch D in the same way. (Details not shown.)

5. Configure MSDP peers:

Configure an MSDP peer on Switch A.

```

[SwitchA] msdp
[SwitchA-msdp] peer 192.168.1.2 connect-interface vlan-interface 101
[SwitchA-msdp] quit

```

Configure MSDP peers on Switch C.

```

[SwitchC] msdp
[SwitchC-msdp] peer 192.168.1.1 connect-interface vlan-interface 101
[SwitchC-msdp] peer 10.110.5.2 connect-interface vlan-interface 104

```

```
[SwitchC-msdp] quit
```

```
# Configure an MSDP peer on Switch D.
```

```
[SwitchD] msdp
```

```
[SwitchD-msdp] peer 10.110.5.1 connect-interface vlan-interface 104
```

```
[SwitchD-msdp] quit
```

6. Configure SA message filtering rules:

```
# Configure an SA message rule on Switch C so that Switch C will not forward SA messages for (Source 1, 225.1.1.0/30) to Switch D.
```

```
[SwitchC] acl number 3001
```

```
[SwitchC-acl-adv-3001] rule deny ip source 10.110.3.100 0 destination 225.1.1.0 0.0.0.3
```

```
[SwitchC-acl-adv-3001] rule permit ip source any destination any
```

```
[SwitchC-acl-adv-3001] quit
```

```
[SwitchC] msdp
```

```
[SwitchC-msdp] peer 10.110.5.2 sa-policy export acl 3001
```

```
[SwitchC-msdp] quit
```

```
# Configure an SA message rule on Switch D so that Switch D will not create SA messages for Source 2.
```

```
[SwitchD] acl number 2001
```

```
[SwitchD-acl-basic-2001] rule deny source 10.110.6.100 0
```

```
[SwitchD-acl-basic-2001] quit
```

```
[SwitchD] msdp
```

```
[SwitchD-msdp] import-source acl 2001
```

```
[SwitchD-msdp] quit
```

Verifying the configuration

Display the (S, G) entries cached in the SA cache on the switches using the **display msdp sa-cache** command. For example:

```
# Display the (S, G) entries cached in the SA cache on Switch C.
```

```
[SwitchC] display msdp sa-cache
```

```
MSDP Source-Active Cache Information of VPN-Instance: public net
```

```
MSDP Total Source-Active Cache - 8 entries
```

```
MSDP matched 8 entries
```

(Source, Group)	Origin RP	Pro	AS	Uptime	Expires
(10.110.3.100, 225.1.1.0)	1.1.1.1	?	?	02:03:30	00:05:31
(10.110.3.100, 225.1.1.1)	1.1.1.1	?	?	02:03:30	00:05:31
(10.110.3.100, 225.1.1.2)	1.1.1.1	?	?	02:03:30	00:05:31
(10.110.3.100, 225.1.1.3)	1.1.1.1	?	?	02:03:30	00:05:31
(10.110.3.100, 226.1.1.0)	1.1.1.1	?	?	02:03:30	00:05:31
(10.110.3.100, 226.1.1.1)	1.1.1.1	?	?	02:03:30	00:05:31
(10.110.3.100, 226.1.1.2)	1.1.1.1	?	?	02:03:30	00:05:31
(10.110.3.100, 226.1.1.3)	1.1.1.1	?	?	02:03:30	00:05:31

```
# Display the (S, G) entries cached in the SA cache on Switch D.
```

```
[SwitchD] display msdp sa-cache
```



```
MSDP Source-Active Cache Information of VPN-Instance: public net
MSDP Total Source-Active Cache - 4 entries
MSDP matched 4 entries
```

(Source, Group)	Origin RP	Pro	AS	Uptime	Expires
(10.110.3.100, 226.1.1.0)	1.1.1.1	?	?	00:32:53	00:05:07
(10.110.3.100, 226.1.1.1)	1.1.1.1	?	?	00:32:53	00:05:07
(10.110.3.100, 226.1.1.2)	1.1.1.1	?	?	00:32:53	00:05:07
(10.110.3.100, 226.1.1.3)	1.1.1.1	?	?	00:32:53	00:05:07

Troubleshooting MSDP

MSDP peers stay in down state

Symptom

The configured MSDP peers stay in the down state.

Analysis

- A TCP connection-based MSDP peering relationship is established between the local interface address and the MSDP peer after the configuration.
- The TCP connection setup will fail if the local interface address is not consistent with the MSDP peer address configured on the peer router.
- If no route is available between the MSDP peers, the TCP connection setup will fail.

Solution

1. Verify that a route is available between the routers. Use the **display ip routing-table** command to determine whether the unicast route between the routers is correct.
2. Verify that a unicast route is available between the two routers that will become MSDP peers to each other.
3. Verify the interface address consistency between the MSDP peers. Use the **display current-configuration** command to verify that the local interface address and the MSDP peer address of the remote router are the same.

No SA entries in the switch's SA cache

Symptom

MSDP fails to send (S, G) entries through SA messages.

Analysis

- The **import-source** command controls sending (S, G) entries through SA messages to MSDP peers. If this command is executed without the *acl-number* argument, all the (S, G) entries are filtered out. That is, no (S, G) entries of the local domain is advertised.

- If the **import-source** command is not executed, the system will advertise all the (S, G) entries of the local domain. If MSDP fails to send (S, G) entries through SA messages, verify that the **import-source** command has been correctly configured.

Solution

1. Use the **display ip routing-table** command to verify that the unicast route between the routers is correct.
2. Verify that a unicast route is available between the two routers that will become MSDP peers to each other.
3. Verify the configuration of the **import-source** command and its *acl-number* argument and be sure that ACL rule can filter appropriate (S, G) entries.

Inter-RP communication faults in Anycast RP application

Symptom

RPs fail to exchange their locally registered (S, G) entries with one another in the Anycast RP application.

Analysis

- In the Anycast RP application, RPs in the same PIM-SM domain are configured to be MSDP peers to achieve load balancing among the RPs.
- An MSDP peer address must be different from the Anycast RP address, and the C-BSR and C-RP must be configured on different devices or interfaces.
- If the **originating-rp** command is executed, MSDP will replace the RP address in the SA messages with the address of the interface specified in the command.
- When an MSDP peer receives an SA message, it performs RPF check on the message. If the MSDP peer finds that the remote RP address is the same as the local RP address, it will discard the SA message.

Solution

1. Use the **display ip routing-table** command to verify that the unicast route between the routers is correct.
2. Verify that a unicast route is available between the two routers that will become MSDP peer to each other.
3. Verify the configuration of the **originating-rp** command. In the Anycast RP application environment, be sure to use the **originating-rp** command to configure the RP address in the SA messages, which must be the local interface address.
4. Verify that the C-BSR address is different from the Anycast RP address.

Configuring MBGP (available only on the HP 5500 EI)

This chapter covers configuration tasks related to multiprotocol BGP for IP multicast only. For more information about BGP, see *Layer 3—IP Routing Configuration Guide*.

The term "router" in this chapter refers to both routers and Layer 3 switches.

MBGP overview

BGP-4 can carry routing information for IPv4 only. IETF defined Multiprotocol Border Gateway Protocol (MP-BGP) to extend BGP-4 so that BGP can carry routing information for multiple network-layer protocols.

For a network, the topology for multicast might be different from that for unicast. To distinguish them, the MP-BGP enables BGP to carry the unicast Network Layer Reachability Information (NLRI) and multicast NLRI separately. The multicast NLRI performs reverse path forwarding (RPF) exclusively. In this way, route selection for a destination through the unicast routing table and through the multicast routing table have different results, ensuring consistent unicast forwarding and normal multicast between domains. For more information about RPF, see "[Configuring multicast routing and forwarding \(available only on the HP 5500 EI\)](#)."

MP-BGP is defined in RFC 2858 (Multiprotocol Extensions for BGP-4). The application of MP-BGP on multicast is called Multicast BGP (MBGP).

Protocols and standards

- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 3392, *Capabilities Advertisement with BGP-4*
- draft-ietf-idmr-bgp-mcast-attr-00, *BGP Attributes for Multicast Tree Construction*
- RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*
- RFC 5291, *Outbound Route Filtering Capability for BGP-4*
- RFC 5292, *Address-Prefix-Based Outbound Route Filter for BGP-4*

MBGP configuration task list

Task	Remarks
Configuring basic MBGP functions	Required

Task		Remarks
Controlling route advertisement and reception	Configuring MBGP route redistribution	Required
	Configuring default route redistribution into MBGP	Optional
	Configuring MBGP route summarization	Optional
	Advertising a default route to an IPv4 MBGP peer or peer group	Optional
	Configuring outbound MBGP route filtering	Optional
	Configuring inbound MBGP route filtering	Optional
	Configuring MBGP route dampening	Optional
Configuring MBGP route attributes	Configuring MBGP route preferences	
	Configuring the default local preference	
	Configuring the MED attribute	Optional
	Configuring the NEXT_HOP attribute	
Tuning and optimizing MBGP networks	Configuring the AS_PATH attributes	
	Configuring MBGP soft reset	Optional
	Enabling the MBGP ORF capability	Optional
Configuring a large scale MBGP network	Configuring the maximum number of MBGP routes for load balancing	Optional
	Configuring IPv4 MBGP peer groups	Optional
	Configuring MBGP community	Optional
	Configuring an MBGP route reflector	Optional

Configuring basic MBGP functions

Before you configure MBGP, be sure that neighboring nodes can access each other at the network layer.

To configure basic MBGP functions:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Specify a peer or peer group and its AS number.	peer { <i>group-name</i> <i>ip-address</i> } as-number <i>as-number</i>	Not specified by default.
4. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
5. Enable a peer or peer group created in IPv4 unicast view.	peer { <i>group-name</i> <i>ip-address</i> } enable	Not enabled by default.
6. Specify a preferred value for routes from an IPv4 MBGP peer or peer group.	peer { <i>group-name</i> <i>ip-address</i> } preferred-value <i>value</i>	Optional. The default preferred value is 0.

Controlling route advertisement and reception

Before configuring this task, configure basic MBGP functions first.

Configuring MBGP route redistribution

MBGP can advertise routing information in the local AS to neighboring ASs. It redistributes such routing information from IGP into its routing table rather than learning the information by itself.

To configure MBGP route redistribution:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
4. Configure MBGP route redistribution.	<p>Enable route redistribution from another routing protocol:</p> <pre>import-route <i>protocol</i> [{ <i>process-id</i> all-processes } [allow-direct med <i>med-value</i> route-policy <i>route-policy-name</i>] *]</pre> <p>Inject a network into the MBGP routing table:</p> <pre>network <i>ip-address</i> [<i>mask</i> <i>mask-length</i>] [short-cut route-policy <i>route-policy-name</i>]</pre>	<p>Use either command</p> <p>No route redistribution is configured by default.</p> <p>The allow-direct keyword is available only when the specified routing protocol is OSPF.</p> <p>The ORIGIN attribute of routes redistributed into the MBGP routing table with the import-route command is Incomplete.</p> <p>The ORIGIN attribute of routes injected into the MBGP routing table with the network command is IGP.</p>

NOTE:

The networks to be injected must exist in the local IP routing table, and using a routing policy makes route control more flexible.

Configuring default route redistribution into MBGP

You cannot use the **import-route** command to redistribute any default route into the MBGP routing table. This task allows you to redistribute default routes in another way.

To configure MBGP to redistribute a default route from another protocol:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A

Step	Command	Remarks
3. Enter MBGP address family view.	ipv4-family multicast	N/A
4. Enable route redistribution from another routing protocol.	import-route protocol [{ <i>process-id</i> all-processes } [allow-direct med med-value route-policy route-policy-name] *]	No route redistribution is configured by default. The allow-direct keyword is available only when the specified routing protocol is OSPF.
5. Enable default route redistribution into the MBGP routing table.	default-route imported	Not enabled by default.

Configuring MBGP route summarization

To reduce the routing table size on medium and large MBGP networks, you need to configure route summarization on peers. MBGP supports automatic and manual summarization modes:

- **Automatic summarization**—Summarizes subnets redistributed from IGP. With the feature configured, MBGP advertises only summary natural networks rather than subnets. The default routes and routes injected with the **network** command are not summarized.
- **Manual summarization**—Summarizes MBGP local routes. A manual summary route has a higher priority than an automatic one.

To configure MBGP route summarization:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp as-number	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
4. Configure MBGP route summarization.	<p>Enable automatic route summarization:</p> <p>summary automatic</p> <p>Configure manual route summarization:</p> <p>aggregate ip-address { <i>mask</i> <i>mask-length</i> } [as-set attribute-policy route-policy-name detail-suppressed origin-policy route-policy-name suppress-policy route-policy-name] *</p>	<p>Use either command</p> <p>No route summarization is configured by default.</p> <p>If the two commands are both configured, the manual route summarization takes effect.</p>

Advertising a default route to an IPv4 MBGP peer or peer group

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
4. Advertise a default route to an MBGP peer or peer group.	peer { <i>group-name</i> <i>ip-address</i> } default-route-advertise [route-policy <i>route-policy-name</i>]	Not advertised by default.

NOTE:

With the **peer default-route-advertise** command executed, the router sends a default route with the next hop as itself to the specified MBGP peer or peer group, whether the default route is available or not in the routing table.

Configuring outbound MBGP route filtering

If several filtering policies are configured, they are applied in the following sequence:

1. **filter-policy export**
2. **peer filter-policy export**
3. **peer as-path-acl export**
4. **peer ip-prefix export**
5. **peer route-policy export**

Only the routes that have passed all the configured policies can be advertised.

To configure BGP route distribution filtering policies:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A

Step	Command	Remarks
4. Configure BGP route distribution filtering policies.	<ul style="list-style-type: none"> Configure the filtering of redistributed routes: filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } export [direct isis <i>process-id</i> ospf <i>process-id</i> rip <i>process-id</i> static] Apply a routing policy to advertisements to an IPv4 MBGP peer or a peer group: peer { <i>group-name</i> <i>peer-address</i> } route-policy <i>route-policy-name</i> export Reference an ACL to filter advertisements to an IPv4 MBGP peer or a peer group: peer { <i>group-name</i> <i>ip-address</i> } filter-policy <i>acl-number</i> export Reference an AS path list to filter route advertisements to an IPv4 MBGP peer or a peer group: peer { <i>group-name</i> <i>ip-address</i> } as-path-acl <i>as-path-acl-number</i> export Reference an IP prefix list to filter route advertisements to an IPv4 MBGP peer or a peer group: peer { <i>group-name</i> <i>ip-address</i> } ip-prefix <i>ip-prefix-name</i> export 	Use at least one command. By default, no outbound route filtering is configured.

Configuring inbound MBGP route filtering

By configuring MBGP route reception filtering policies, you can filter out unqualified routes from an MBGP peer or peer group. Members of a peer group can have different route reception filtering policies from the peer group.

If several filtering policies are configured, they are applied in the following sequence:

- filter-policy import**
- peer filter-policy import**
- peer as-path-acl import**
- peer ip-prefix import**
- peer route-policy import**

Only the routes that have passed all the configured policies can be advertised.

To configure MBGP route reception filtering policies:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
4. Configure MBGP route reception filtering policies.	<ul style="list-style-type: none"> Filter incoming routes using an ACL or IP prefix list: filter-policy { <i>acl-number</i> ip-prefix <i>ip-prefix-name</i> } import Reference a routing policy to routes from an IPv4 MBGP peer or a peer group: peer { <i>group-name</i> <i>ip-address</i> } route-policy <i>policy-name</i> import Reference an ACL to filter routing information from an IPv4 MBGP peer or a peer group: peer { <i>group-name</i> <i>ip-address</i> } filter-policy <i>acl-number</i> import Reference an AS path list to filter routing information from an IPv4 MBGP peer or a peer group: peer { <i>group-name</i> <i>ip-address</i> } as-path-acl <i>as-path-acl-number</i> import Reference an IP prefix list to filter routing information from an IPv4 MBGP peer or a peer group: peer { <i>group-name</i> <i>ip-address</i> } ip-prefix <i>ip-prefix-name</i> import 	Use at least one command By default, no inbound route filtering is configured.
5. Specify the maximum number of routes that can be received from an IPv4 MBGP peer or a peer group.	peer { <i>group-name</i> <i>ip-address</i> } route-limit <i>limit</i> [<i>percentage</i>]	Optional The number is unlimited by default.

Configuring MBGP route dampening

By configuring MBGP route dampening, you can suppress unstable routes from being added to the MBGP routing table or being advertised to MBGP peers.

To configure BGP route dampening:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
4. Configure BGP route dampening parameters.	dampening [<i>half-life-reachable</i> <i>half-life-unreachable reuse</i> <i>suppress ceiling</i> route-policy <i>route-policy-name</i>] *	Not configured by default.

Configuring MBGP route attributes

You can modify MBGP route attributes to affect route selection.

Before you configure this task, configure basic MBGP functions first.

Configuring MBGP route preferences

You can reference a routing policy to set preferences for routes matching it. Routes not matching it use the default preferences.

To configure MBGP route preferences:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
4. Configure preferences for external, internal, and local MBGP routes.	preference { <i>external-preference</i> <i>internal-preference</i> <i>local-preference</i> route-policy <i>route-policy-name</i> }	Optional. The default preferences of multicast MBGP EBGp, MBGP IBGP, and local MBGP routes are 255, 255, and 130, respectively.

Configuring the default local preference

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
4. Configure the default local preference.	default local-preference <i>value</i>	Optional. 100 by default.

Configuring the MED attribute

When other conditions of routes to a destination are identical, the route with the smallest MED is selected.

To configure the MED attribute:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
4. Configure the default MED value.	default med <i>med-value</i>	Optional. 0 by default.
5. Enable the comparison of the MED of routes from different ASs.	compare-different-as-med	Optional. Not enabled by default.
6. Enable the comparison of the MED of routes from each AS.	bestroute compare-med	Optional. Not enabled by default.
7. Enable the comparison of the MED of routes from confederation peers.	bestroute med-confederation	Optional. Not enabled by default.

Configuring the NEXT_HOP attribute

You can use the **peer next-hop-local** command to specify the local router as the next hop of routes sent to an MBGP IBGP peer or peer group. If load balancing is configured, the router specifies itself as the next hop of route advertisements to the multicast IBGP peer or peer group regardless of whether the **peer next-hop-local** command is configured.

In a broadcast network where the local router has two multicast EBGp peers, the router does not specify itself as the next hop of routing information sent to the EBGp peers by default unless the **peer next-hop-local** command is configured.

To specify the router as the next hop of routes sent to a peer or a peer group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A

Step	Command	Remarks
4. Specify the router as the next hop of routes sent to a peer or a peer group.	peer { <i>group-name</i> <i>ip-address</i> } next-hop-local	Optional. By default, IPv6 MBGP specifies the local router as the next hop for routes sent to an EBGP peer or a peer group, but not for routes sent to an MBGP IBGP peer or a peer group.

Configuring the AS_PATH attributes

In general, MBGP checks whether the AS_PATH attribute of a route from a peer contains the local AS number. If it does, it discards the route to avoid routing loops.

To configure the AS_PATH attributes:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
4. Allow the local AS number to appear in the AS_PATH of routes from a peer or a peer group and specify the number of times that the local AS number can appear in the AS_PATH of routes from the peer or the peer group.	peer { <i>group-name</i> <i>ip-address</i> } allow-as-loop [<i>number</i>]	Optional. By default, the local AS number cannot appear in routes from a peer or a peer group.
5. Disable BGP from considering the AS_PATH during best route selection.	bestroute as-path-neglect	Optional. By default, BGP considers AS_PATH during best route selection.
6. Configure updates to a peer or a peer group not to keep private AS numbers.	peer { <i>group-name</i> <i>ip-address</i> } public-as-only	Optional. By default, BGP updates carry private AS numbers.

Tuning and optimizing MBGP networks

This task involves resetting MBGP connections and configuring load balancing.

Before configuring this task, configure basic MBGP functions first.

Configuring MBGP soft reset

After modifying a route selection policy, you have to reset MBGP connections to make it take effect.

The current MBGP implementation supports the route refresh feature that enables dynamic route refresh without terminating MBGP connections.

However, if a peer that does not support route refresh exists in the network, you must configure the **peer keep-all-routes** command to save all routes from the peer. When the routing policy is changed, the system updates the MBGP routing table and applies the new policy.

Performing soft reset through route refresh

If the peer is enabled with route refresh, when the MBGP route selection policy is modified on a router, the router advertises a route-refresh message to its MBGP peers, which resend their routing information to the router after receiving the message. Therefore, the local router can perform dynamic route update and apply the new policy without terminating MBGP connections.

To perform soft reset through route refresh:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enable BGP route refresh for a peer or a peer group.	peer { <i>group-name</i> <i>ip-address</i> } capability-advertise route-refresh	Optional. Enabled by default.

Performing soft reset manually

If the peer does not support route refresh, you can use the **peer keep-all-routes** command to save all the route updates from the peer, and then use the **refresh bgp ipv4 multicast** command to soft-reset MBGP connections to refresh the MBGP routing table and apply the new policy without terminating MBGP connections.

To perform a manual soft reset:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Disable BGP route refresh and multiprotocol extensions for a peer or a peer group.	peer { <i>group-name</i> <i>ip-address</i> } capability-advertise conventional	Optional. Enabled by default.
4. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
5. Keep all original routes from a peer or a peer group regardless of whether they pass the inbound filtering policies.	peer { <i>group-name</i> <i>ip-address</i> } keep-all-routes	Not kept by default.
6. Return to user view.	return	N/A

Step	Command	Remarks
7. Soft-reset MBGP connections manually.	refresh bgp ipv4 multicast { all <i>ip-address</i> group <i>group-name</i> external internal } { export import }	Optional.

Enabling the MBGP ORF capability

The MBGP Outbound Router Filter (ORF) feature enables an MBGP speaker to send a set of ORFs to its MBGP peer through route-refresh messages. The peer then applies the ORFs, in addition to its local routing policies (if any), to filter updates to the MBGP speaker, reducing update messages and saving network resources.

After you enable the BGP ORF capability, the local BGP router negotiates the ORF capability with the BGP peer through Open messages. That is, the BGP router determines whether to carry ORF information in messages and, if so, whether to carry nonstandard ORF information in the packets. After completing the negotiation process and establishing the neighboring relationship, the BGP router and its BGP peer can exchange ORF information through specific route-refresh messages.

For the parameters configured on both sides for ORF capability negotiation, see [Table 7](#).

To enable the MBGP ORF capability:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enable BGP route refresh for a peer or a peer group.	peer { <i>group-name</i> <i>ip-address</i> } capability-advertise route-refresh	Optional. Enabled by default. If this feature is not enabled, you need to configure this command. For more information about the command, see <i>Layer 3—IP Routing Command Reference</i> .
4. Enable the non-standard BGP ORF capability for a BGP peer or a peer group.	peer { <i>group-name</i> <i>ipv6-address</i> } capability-advertise orf non-standard	Optional. By default, standard BGP ORF capability defined in RFC 5291 and RFC 5292 is supported. If this feature is not enabled, you need to configure this command. For more information about the command, see <i>Layer 3—IP Routing Command Reference</i> .
5. Enter MBGP address family view.	ipv4-family multicast	N/A

Step	Command	Remarks
6. Enable the ORF IP prefix negotiation capability for an MBGP peer or a peer group.	peer { <i>group-name</i> <i>ip-address</i> } capability-advertise orf ip-prefix { both receive send }	Optional. Not enabled by default.

Table 7 Description of the both, send, and receive parameters and the negotiation result

Local parameter	Peer parameter	Negotiation result
send	<ul style="list-style-type: none"> • receive • both 	The ORF sending capability is enabled locally and the ORF receiving capability is enabled on the peer.
receive	<ul style="list-style-type: none"> • send • both 	The ORF receiving capability is enabled locally and the ORF sending capability is enabled on the peer.
both	both	Both the ORF sending and receiving capabilities are enabled locally and on the peer, respectively.

Configuring the maximum number of MBGP routes for load balancing

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
4. Configure the maximum number of MBGP routes for load balancing.	balance <i>number</i>	Not configured by default.

Configuring a large scale MBGP network

Before you configure this task, you must make peering nodes accessible to each other at the network layer.

Configuring IPv4 MBGP peer groups

In a large-scale network, configuration and maintenance become difficult because of large numbers of MBGP peers. You can configure peer groups to make management easier and improve route distribution efficiency.

! IMPORTANT:

- To configure an MBGP peer group, you must enable the corresponding IPv4 BGP unicast peer group in IPv4 MBGP address family view.
- Before adding an MBGP peer to an MBGP peer group, you must add the corresponding IPv4 unicast peer to the IPv4 BGP peer group.

To configure an IPv4 MBGP peer group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp as-number	N/A
3. Create a BGP peer group.	group group-name [external internal]	Not created by default.
4. Add a peer into the peer group.	peer ip-address group group-name [as-number as-number]	No peer is added by default.
5. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
6. Enable the IPv4 unicast peer group.	peer group-name enable	N/A
7. Add an IPv4 MBGP peer to the peer group.	peer ip-address group group-name	Not configured by default.

Configuring MBGP community

The COMMUNITY attribute can be advertised between MBGP peers in different ASs. Routers in the same community share the same policy.

You can reference a routing policy to modify the COMMUNITY attribute for routes sent to a peer. In addition, you can define extended community attributes as needed.

When you configure MBGP community, you must reference a routing policy to define the specific COMMUNITY attributes, and apply the routing policy for route advertisement. For routing policy configuration, see *Layer 3—IP Routing Configuration Guide*.

To configure MBGP community:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp as-number	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A

Step	Command	Remarks
4. Advertise the COMMUNITY attribute to an MBGP peer or a peer group.	<ul style="list-style-type: none"> Advertise the COMMUNITY attribute to an MBGP peer or a peer group: peer { group-name ip-address } advertise-community Advertise the extended community attribute to an MBGP peer or a peer group: peer { group-name ip-address } advertise-ext-community 	Use either command Not configured by default.
5. Apply a routing policy to routes advertised to an MBGP peer or a peer group.	peer { group-name ip-address } route-policy route-policy-name export	Not configured by default.

Configuring an MBGP route reflector

To guarantee the connectivity between multicast IBGP peers in an AS, you need to make them fully meshed. But this becomes unpractical when large numbers of multicast IBGP peers exist. Configuring route reflectors can solve this problem.

In general, it is not required that clients of a route reflector be fully meshed. The route reflector forwards routing information between clients. If clients are fully meshed, you can disable route reflection between clients to reduce routing costs.

In general, a cluster has only one route reflector, and the router ID of the route reflector identifies the cluster. You can configure multiple route reflectors to improve network stability. In this case, you need to specify the same cluster ID for these route reflectors to avoid routing loops.

To configure an MBGP route reflector:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp as-number	N/A
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	N/A
4. Configure the router as a route reflector and specify an MBGP peer or a peer group as its client.	peer { group-name peer-address } reflect-client	Not configured by default.
5. Enable route reflection between clients.	reflect between-clients	Optional. Enabled by default.
6. Configure the cluster ID of the route reflector.	reflector cluster-id cluster-id	Optional. By default, a route reflector uses its router ID as the cluster ID.

Displaying and maintaining MBGP

Displaying MBGP

Task	Command	Remarks
Display the IPv4 MBGP routing table.	display ip multicast routing-table [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the IPv4 MBGP routing information matching the specified destination IP address.	display ip multicast routing-table <i>ip-address</i> [<i>mask-length</i> <i>mask</i>] [longer-match] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display MBGP peer group information.	display bgp multicast group [<i>group-name</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the advertised networks.	display bgp multicast network [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display AS path information.	display bgp multicast paths [<i>as-regular-expression</i> { begin exclude include } <i>regular-expression</i>]	Available in any view
Display MBGP peer information or peer group information.	display bgp multicast peer [[<i>ip-address</i>] verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the prefix entries in the ORF information from the specified BGP peer.	display bgp multicast peer <i>ip-address</i> received ip-prefix [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display MBGP routing information.	display bgp multicast routing-table [<i>ip-address</i> [{ <i>mask</i> <i>mask-length</i> }] [longer-prefixes]] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display MBGP routing information matching the AS path list.	display bgp multicast routing-table as-path-acl <i>as-path-acl-number</i> [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display MBGP CIDR routing information.	display bgp multicast routing-table cidr [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display MBGP routing information matching the specified BGP community.	display bgp multicast routing-table community [<i>aa:nn&<1-13></i>] [no-advertise no-export no-export-subconfed] * [whole-match] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display MBGP routing information matching an MBGP community list.	display bgp multicast routing-table community-list { { <i>basic-community-list-number</i> <i>comm-list-name</i> } [whole-match] <i>adv-community-list-number</i> } [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display MBGP dampened routing information.	display bgp multicast routing-table dampened [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display MBGP dampening parameter information.	display bgp multicast routing-table dampening parameter [{ begin exclude include } <i>regular-expression</i>]	Available in any view

Task	Command	Remarks
Display MBGP routing information originating from different ASs.	display bgp multicast routing-table different-origin-as [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv4 MBGP routing flap statistics.	display bgp multicast routing-table flap-info [regular-expression <i>as-regular-expression</i> [as-path-acl <i>as-path-acl-number</i> <i>ip-address</i> [{ <i>mask</i> <i>mask-length</i> } [longer-match]]] [{ begin exclude include } <i>regular-expression</i>]]	Available in any view
Display IPv4 MBGP routing information sent to or received from an MBGP peer.	display bgp multicast routing-table peer <i>ip-address</i> { advertised-routes received-routes } [<i>network-address</i> [<i>mask</i> <i>mask-length</i>] statistic] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv4 MBGP routing information matching an AS regular expression.	display bgp multicast routing-table regular-expression <i>as-regular-expression</i>	Available in any view
Display IPv4 MBGP routing statistics.	display bgp multicast routing-table statistic [{ begin exclude include } <i>regular-expression</i>]	Available in any view

Resetting MBGP connections

Task	Command	Remarks
Reset specified MBGP connections.	reset bgp ipv4 multicast { all <i>as-number</i> <i>ip-address</i> group <i>group-name</i> external internal }	Available in user view

Clearing MBGP information

Task	Command	Remarks
Clear dampened routing information and release suppressed routes.	reset bgp ipv4 multicast dampening [<i>ip-address</i> [<i>mask</i> <i>mask-length</i>]]	Available in user view
Clear MBGP route flap statistics.	reset bgp ipv4 multicast flap-info [regexp <i>as-path-regexp</i> as-path-acl <i>as-path-acl-number</i> <i>ip-address</i> [<i>mask</i> <i>mask-length</i>]]	Available in user view

MBGP configuration example

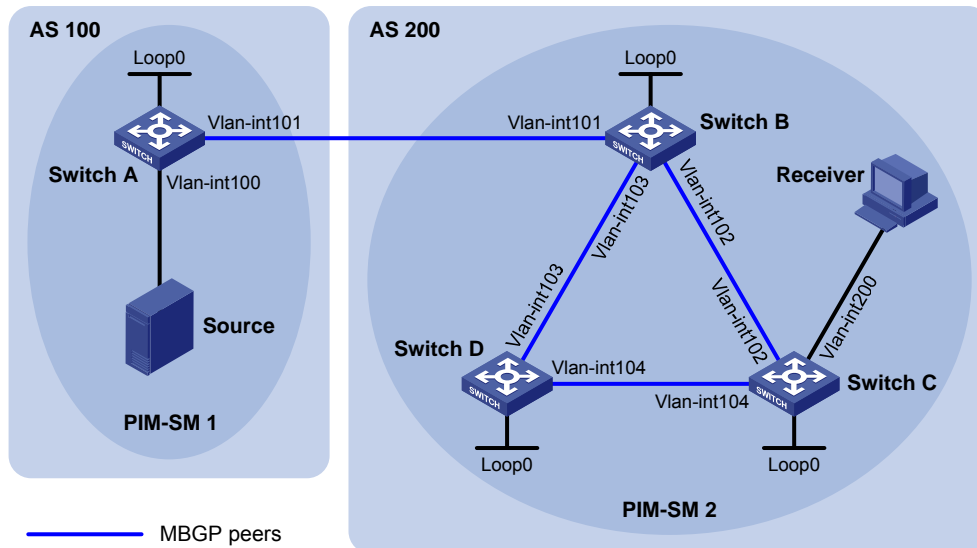
Network requirements

As shown in the following figure:

- PIM-SM 1 is in AS 100, and PIM-SM 2 is in AS 200. OSPF is the IGP in the two ASs, and MBGP runs between the two ASs to exchange multicast route information.
- The multicast source belongs to PIM-SM 1, and the receiver belongs to PIM-SM 2.

- Configure the respective Loopback 0 of Switch A and Switch B as the C-BSR and C-RP of the respective PIM-SM domains.
- Set up an MSDP peer relationship between Switch A and Switch B through MBGP.

Figure 66 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Source	N/A	10.110.1.100/24	Switch C	Vlan-int200	10.110.2.1/24
Switch A	Vlan-int100	10.110.1.1/24	Switch C	Vlan-int102	192.168.2.2/24
	Vlan-int101	192.168.1.1/24		Vlan-int104	192.168.4.1/24
	Loop0	1.1.1.1/32	Switch C	Loop0	3.3.3.3/32
Switch B	Vlan-int101	192.168.1.2/24	Switch D	Vlan-int103	192.168.3.2/24
	Vlan-int102	192.168.2.1/24		Vlan-int104	192.168.4.2/24
	Vlan-int103	192.168.3.1/24	Switch D	Loop0	4.4.4.4/32
Switch B	Loop0	2.2.2.2/32			

Configuration procedure

1. Configure IP addresses for interfaces. (Details not shown.)
2. Configure OSPF. (Details not shown.)
3. Enable IP multicast routing, PIM-SM and IGMP, and configure a PIM-SM domain border:

Enable IP multicast routing on Switch A, and enable PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
```

The configuration on Switch B and Switch D is similar to the configuration on Switch A.

Enable IP multicast routing on Switch C, enable PIM-SM on each interface, and enable IGMP on the host-side interface VLAN-interface 200.

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 102
[SwitchC-Vlan-interface102] pim sm
[SwitchC-Vlan-interface102] quit
[SwitchC] interface vlan-interface 104
[SwitchC-Vlan-interface104] pim sm
[SwitchC-Vlan-interface104] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] pim sm
[SwitchC-Vlan-interface200] igmp enable
[SwitchC-Vlan-interface200] quit
```

Configure a PIM domain border on Switch A.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim bsr-boundary
[SwitchA-Vlan-interface101] quit
```

Configure a PIM domain border on Switch B.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim bsr-boundary
[SwitchB-Vlan-interface101] quit
```

4. Configure Loopback 0 and the position of C-BSR, and C-RP:

Configure Loopback 0 and configure it as the C-BSR and C-RP on Switch A.

```
[SwitchA] interface loopback 0
[SwitchA-LoopBack0] ip address 1.1.1.1 32
[SwitchA-LoopBack0] pim sm
[SwitchA-LoopBack0] quit
[SwitchA] pim
[SwitchA-pim] c-bsr loopback 0
[SwitchA-pim] c-rp loopback 0
[SwitchA-pim] quit
```

Configure Loopback 0 and configure it as the C-BSR and C-RP on Switch B.

```
[SwitchB] interface loopback 0
[SwitchB-LoopBack0] ip address 2.2.2.2 32
[SwitchB-LoopBack0] pim sm
[SwitchB-LoopBack0] quit
[SwitchB] pim
[SwitchB-pim] c-bsr loopback 0
[SwitchB-pim] c-rp loopback 0
[SwitchB-pim] quit
```

5. Configure BGP, specify the MBGP peer and enable direct route redistribution:

On Switch A, configure the MBGP peer and enable direct route redistribution.

```
[SwitchA] bgp 100
[SwitchA-bgp] router-id 1.1.1.1
```

```
[SwitchA-bgp] peer 192.168.1.2 as-number 200
[SwitchA-bgp] import-route direct
[SwitchA-bgp] ipv4-family multicast
[SwitchA-bgp-af-mul] peer 192.168.1.2 enable
[SwitchA-bgp-af-mul] import-route direct
[SwitchA-bgp-af-mul] quit
[SwitchA-bgp] quit
```

On Switch B, configure the MBGP peer and enable route redistribution from OSPF.

```
[SwitchB] bgp 200
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 192.168.1.1 as-number 100
[SwitchB-bgp] import-route ospf 1
[SwitchB-bgp] ipv4-family multicast
[SwitchB-bgp-af-mul] peer 192.168.1.1 enable
[SwitchB-bgp-af-mul] import-route ospf 1
[SwitchB-bgp-af-mul] quit
[SwitchB-bgp] quit
```

6. Configure MSDP peer:

Specify the MSDP peer on Switch A.

```
[SwitchA] msdp
[SwitchA-msdp] peer 192.168.1.2 connect-interface vlan-interface 101
[SwitchA-msdp] quit
```

Specify the MSDP peer on Switch B.

```
[SwitchB] msdp
[SwitchB-msdp] peer 192.168.1.1 connect-interface vlan-interface 101
[SwitchB-msdp] quit
```

7. Verify the configuration:

Use the **display bgp multicast peer** command to display MBGP peers on a switch. For example:

Display MBGP peers on Switch B.

```
[SwitchB] display bgp multicast peer
```

```
BGP local router ID : 2.2.2.2
Local AS number : 200
Total number of peers : 3                Peers in established state : 3
```

Peer	AS	MsgRcvd	MsgSent	OutQ	PrefRcv	Up/Down	State
192.168.1.1	100	56	56	0	0	00:40:54	Established

Use the **display msdp brief** command to display MSDP peers on a switch. For example:

Display brief information about MSDP peers on Switch B.

```
[SwitchB] display msdp brief
```

MSDP Peer Brief Information of VPN-Instance: public net

Configured	Up	Listen	Connect	Shutdown	Down
1	1	0	0	0	0
Peer's Address	State	Up/Down time	AS	SA Count	Reset Count

192.168.1.1	Up	00:07:17	100	1	0
-------------	----	----------	-----	---	---

Configuring MLD snooping

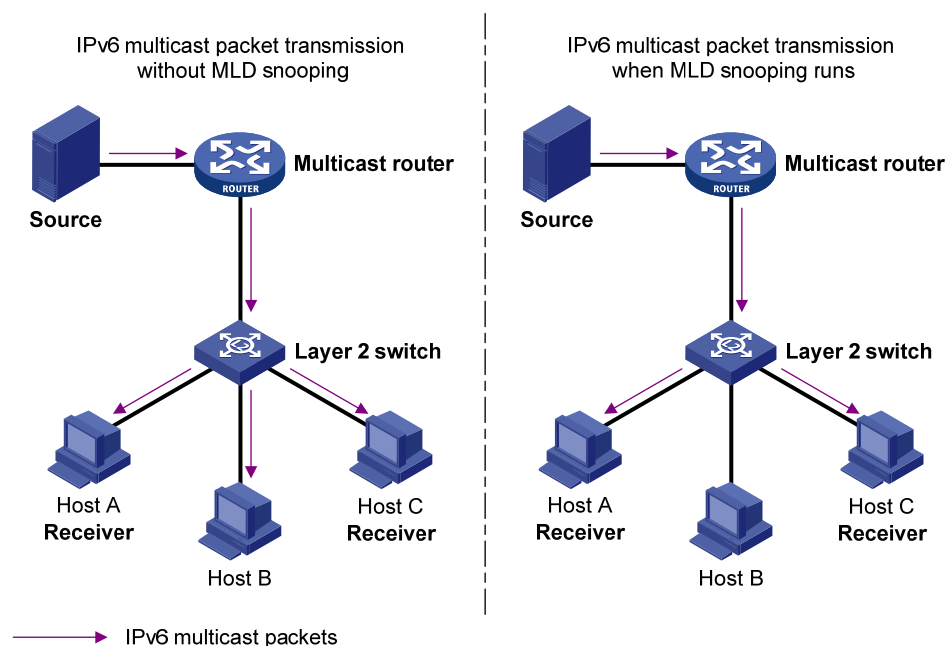
Overview

Multicast Listener Discovery (MLD) snooping is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups.

By analyzing received MLD messages, a Layer 2 device that runs MLD snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.

As shown in [Figure 67](#), without MLD snooping enabled, the Layer 2 switch floods IPv6 multicast packets to all devices at Layer 2. With MLD snooping enabled, the Layer 2 switch forwards IPv6 multicast packets destined for known IPv6 multicast groups to only the receivers that require the multicast data at Layer 2. This feature improves bandwidth efficiency, enhances multicast security, and helps per-host accounting for multicast users.

Figure 67 Before and after MLD snooping is enabled on the Layer 2 device

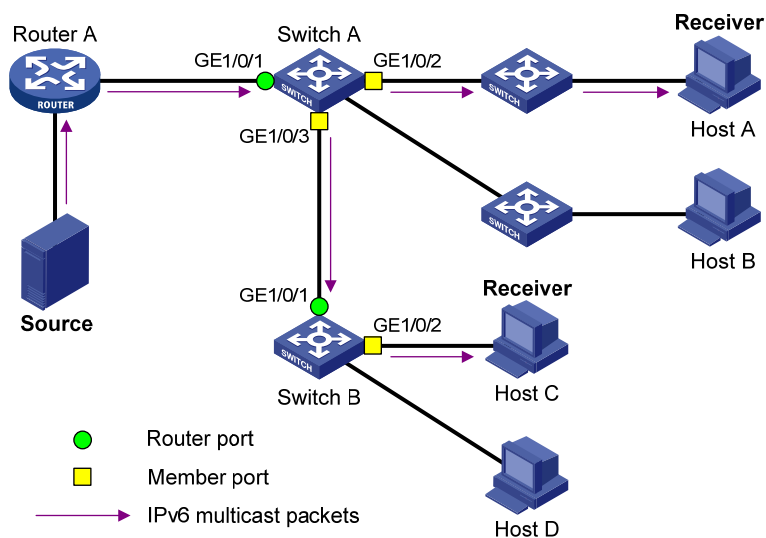


Basic concepts in MLD snooping

MLD snooping related ports

As shown in [Figure 68](#), Router A connects to the multicast source, MLD snooping runs on Switch A and Switch B, and Host A and Host C are receiver hosts as members of an IPv6 multicast group.

Figure 68 MLD snooping related ports



Ports involved in MLD snooping, as shown in Figure 68, are described as follows:

- Router port**—Layer 3 multicast device-side port. Layer 3 multicast devices include designated routers (DRs) and MLD querier. In the figure, GigabitEthernet 1/0/1 of Switch A and GigabitEthernet 1/0/1 of Switch B are router ports. The switch registers all its router ports in its router port list.

Do not confuse the "router port" in MLD snooping with the "routed interface" commonly known as the "Layer 3 interface." The router port in MLD snooping is the Layer 2 interface.
- Member port**—Multicast receiver-side port. In the figure, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and GigabitEthernet 1/0/2 of Switch B are member ports. The switch registers all its member ports in its MLD snooping forwarding table.

Unless otherwise specified, router ports and member ports in this document include both static and dynamic router ports and member ports.

NOTE:

An MLD snooping-enabled switch deems that the all its ports that receive MLD general queries with the source address other than 0::0 or that receive IPv6 PIM hello messages are dynamic router ports. For more information about IPv6 PIM hello messages, see "[Configuring IPv6 PIM \(available only on the HP 5500 EI\)](#)."

Aging timers for dynamic ports in MLD snooping and related messages and actions

Timer	Description	Message before expiry	Action after expiry
Dynamic router port aging timer	For each dynamic router port, the switch starts an aging timer. When the timer expires, the dynamic router port ages out.	MLD general query of which the source address is not 0::0 or IPv6 PIM hello.	The switch removes this port from its router port list.

Timer	Description	Message before expiry	Action after expiry
Dynamic member port aging timer	When a port dynamically joins a multicast group, the switch starts an aging timer for the port. When the timer expires, the dynamic member port ages out.	MLD report message.	The switch removes this port from the MLD snooping forwarding table.

NOTE:

In MLD snooping, only dynamic ports age out. Static ports never age out.

How MLD snooping works

In this section, the involved ports are dynamic ports. For information about how to configure and remove static ports, see "[Configuring static ports.](#)"

A switch that runs MLD snooping performs different actions when it receives different MLD messages, as follows:

When receiving a general query

The MLD querier periodically sends MLD general queries to all hosts and routers identified by the IPv6 address FF02::1 on the local subnet to determine whether any active IPv6 multicast group members exist on the subnet.

After receiving an MLD general query, the switch forwards it to all ports in the VLAN, except the port that received the query. The switch also performs one of the following actions:

- If the receiving port is a dynamic router port in the router port list, restarts the aging timer for the port.
- If the receiving port is not in the router port list, adds it into the router port list as a dynamic router port and starts an aging timer for the port.

When receiving a membership report

A host sends an MLD report to the MLD querier for the following purposes:

- If the host has been a member of an IPv6 multicast group, responds to the query with an MLD report.
- Applies for joining an IPv6 multicast group.

After receiving an MLD report, the switch forwards it through all the router ports in the VLAN, resolves the address of the reported IPv6 multicast group, and performs one of the following actions:

- If no forwarding entry matches the group address, creates a forwarding entry for the group, adds the receiving port as a dynamic member port to the forwarding entry for the group, and starts an aging timer for the port.
- If a forwarding entry matches the group address, but the receiving port is not in the forwarding entry for the group, adds the port as a dynamic member port to the forwarding entry, and starts an aging timer for the port.

- If a forwarding entry matches the group address and the receiving port is in the forwarding entry for the group, restarts the aging timer for the port.

A switch does not forward an MLD report through a non-router port. If the switch forwards a report message through a member port, the MLD report suppression mechanism causes all the attached hosts that monitor the reported IPv6 multicast address suppress their own reports. This makes the switch unable to know whether the reported multicast group still has active members attached to that port.

For more information about the MLD report suppression mechanism of hosts, see "[Configuring MLD \(available only on the HP 5500 EI\)](#)."

When receiving a done message

When a host leaves an IPv6 multicast group, the host sends an MLD done message to the multicast routers. When the switch receives the MLD done message on a dynamic member port, the switch first checks whether a forwarding entry matches the IPv6 multicast group address in the message, and, if a match is found, whether the forwarding entry contains the dynamic member port.

- If no forwarding entry matches the IPv6 multicast group address, or if the forwarding entry does not contain the port, the switch directly discards the MLD done message.
- If a forwarding entry matches the IPv6 multicast group address and contains the port, the switch forwards the done message to all router ports in the native VLAN. Because the switch does not know whether any other hosts attached to the port are still listening to that IPv6 multicast group address, the switch does not immediately remove the port from the forwarding entry for that group. Instead, it restarts the aging timer for the port.

After receiving the MLD done message, the MLD querier resolves the IPv6 multicast group address in the message and sends an MLD multicast-address-specific query to that IPv6 multicast group through the port that received the MLD done message. After receiving the MLD multicast-address-specific query, the switch forwards it through all its router ports in the VLAN and all member ports of the IPv6 multicast group. The switch also performs the following judgment for the port that received the MLD done message:

- If the port (assuming that it is a dynamic member port) receives an MLD report in response to the MLD multicast-address-specific query before its aging timer expires, it indicates that some host attached to the port is receiving or expecting to receive IPv6 multicast data for that IPv6 multicast group. The switch restarts the aging timer for the port.
- If the port receives no MLD report in response to the MLD multicast-address-specific query before its aging timer expires, it indicates that no hosts attached to the port are still monitoring that IPv6 multicast group address. The switch removes the port from the forwarding entry for the IPv6 multicast group when the aging timer expires.

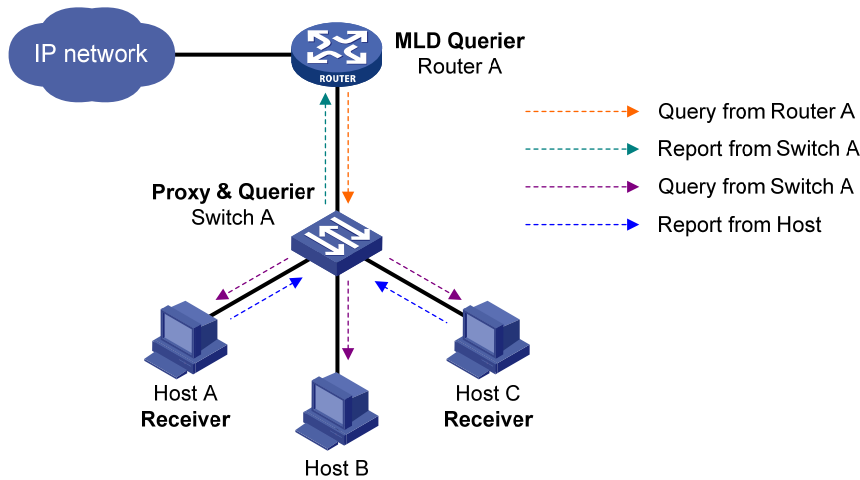
MLD snooping proxying

You can configure the MLD snooping proxying function on an edge device to reduce the number of MLD reports and done messages sent to its upstream device. The device configured with MLD snooping proxying is called an MLD snooping proxy. It is a host from the perspective of its upstream device.

NOTE:

Even though an MLD snooping proxy is a host from the perspective of its upstream device, the MLD membership report suppression mechanism for hosts does not take effect on it. For more information about the MLD report suppression mechanism for hosts, see "[Configuring MLD \(available only on the HP 5500 EI\)](#)."

Figure 69 Network diagram



As shown in [Figure 69](#), Switch A works as an MLD snooping proxy. As a host from the perspective of the querier Router A, Switch A represents its attached hosts to send their membership reports and done messages to Router A.

[Table 8](#) describes how an MLD snooping proxy processes MLD messages.

Table 8 MLD message processing on an MLD snooping proxy

MLD message	Actions
General query	When receiving an MLD general query, the proxy forwards it to all ports but the receiving port. In addition, the proxy generates a report according to the group memberships that it maintains and sends the report out of all router ports.
Multicast-address-specific query	In response to the MLD group-specific query for a certain IPv6 multicast group, the proxy sends the report to the group out of all router ports if the forwarding entry for the group still contains a member port.
Report	<p>When receiving a report for an IPv6 multicast group, the proxy looks up the multicast forwarding table for the entry for the multicast group.</p> <ul style="list-style-type: none">• If a forwarding entry matches the IPv6 multicast group, and contains the receiving port as a dynamic member port, the proxy restarts the aging timer for the port.• If a forwarding entry matches the IPv6 multicast group but does not contain the receiving port, the proxy adds the port to the forwarding entry as a dynamic member port and starts an aging timer for the port.• If no forwarding entry matches the IPv6 multicast group, the proxy creates a forwarding entry for the group, adds the receiving port to the forwarding entry as a dynamic member port, and starts an aging timer for the port. <p>Then, the switch sends the report to the group out of all router ports.</p>

MLD message	Actions
Done	In response to a done message for an IPv6 multicast group, the proxy sends a multicast-address-specific query for the group out of the receiving port. After making sure that no member port is contained in the forwarding entry for the IPv6 multicast group, the proxy sends a done message for the group out of all router ports.

Protocols and standards

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

MLD snooping configuration task list

Task	Remarks	
Configuring basic MLD snooping functions	Enabling MLD snooping	Required
	Specifying the version of MLD snooping	Optional
	Configuring IPv6 static multicast MAC address entries	Optional
Configuring MLD snooping port functions	Configuring aging timers for dynamic ports	Optional
	Configuring static ports	Optional
	Configuring a port as a simulated member host	Optional
	Enabling fast-leave processing	Optional
	Disabling a port from becoming a dynamic router port	Optional
Configuring MLD snooping querier	Enabling MLD snooping querier	Optional
	Configuring parameters for MLD queries and responses	Optional
	Configuring the source IPv6 addresses for MLD queries	Optional
Configuring MLD snooping proxying	Enabling MLD snooping proxying	Optional
	Configuring the source IPv6 addresses for the MLD messages sent by the proxy	Optional
Configuring an MLD snooping policy	Configuring an IPv6 multicast group filter	Optional
	Configuring IPv6 multicast source port filtering	Optional
	Enabling dropping unknown IPv6 multicast data	Optional
	Configuring MLD report suppression	Optional
	Setting the maximum number of multicast groups that a port can join	Optional
	Enabling IPv6 multicast group replacement	Optional
	Setting the 802.1p precedence for MLD messages	Optional
	Configuring an IPv6 multicast user control policy	Optional
	Enabling the MLD snooping host tracking function	Optional
Setting the DSCP value for MLD messages	Optional	

For the configuration tasks in this section:

- In MLD-snooping view, the configurations that you make are effective in all VLANs . In VLAN view, the configurations that you make are effective only on the ports that belong to the current VLAN. For a given VLAN, a configuration that you make in MLD-snooping view is effective only if you do not make the same configuration in VLAN view.
- In MLD-snooping view, the configurations that you make are effective on all ports. In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the configurations that you make are effective only on the current port. In port group view, the configurations that you make are effective on all ports in only the current port group. For a given port, a configuration that you make in MLD-snooping view is effective only if you do not make the same configuration in Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.
- For MLD snooping, the configurations that you make on a Layer 2 aggregate interface do not interfere with those made on its member ports, nor do they participate in aggregation calculations. Configurations that you make on a member port of the aggregate group will not take effect until the port leaves the aggregate group.

Configuring basic MLD snooping functions

Before you configure basic MLD snooping functions, complete the following tasks:

- Enable IPv6 forwarding.
- Configure the corresponding VLANs.
- Determine the version of MLD snooping.

Enabling MLD snooping

When you enable MLD snooping, follow these guidelines:

- You must enable MLD snooping globally before you enable it for a VLAN.
- After you enable MLD snooping for a VLAN, you cannot enable MLD or IPv6 PIM on the corresponding VLAN interface, and vice versa.
- MLD snooping for a VLAN works only on the ports in this VLAN.

To enable MLD snooping:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable MLD snooping globally and enter MLD-snooping view.	mld-snooping	Disabled by default
3. Return to system view.	quit	N/A
4. Enter VLAN view.	vlan <i>vlan-id</i>	N/A

Step	Command	Remarks
5. Enable MLD snooping for the VLAN.	mld-snooping enable	Disabled by default

Specifying the version of MLD snooping

Different versions of MLD snooping can process different versions of MLD messages:

- MLDv1 snooping can process MLDv1 messages, but flood MLDv2 messages in the VLAN instead of processing them.
- MLDv2 snooping can process MLDv1 and MLDv2 messages.

If you change MLDv2 snooping to MLDv1 snooping, the system:

- Clears all MLD snooping forwarding entries that are dynamically created.
- Keeps static MLDv2 snooping forwarding entries (*, G).
- Clears static MLDv2 snooping forwarding entries (S, G), which will be restored when MLDv1 snooping is changed back to MLDv2 snooping.

For more information about static joining, see "[Configuring static ports.](#)"

Configuration procedure

To specify the version of MLD snooping:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Specify the version of MLD snooping.	mld-snooping version <i>version-number</i>	Version 1 by default

Configuring IPv6 static multicast MAC address entries

In Layer-2 multicast, a Layer-2 IPv6 multicast protocol (such as MLD snooping) can dynamically add IPv6 multicast MAC address entries. Or, you can manually configure IPv6 multicast MAC address entries.

Configuration guidelines

- The configuration that you make in system view is effective on the specified interfaces. The configuration that you make in interface view or port group view is effective only on the current interface or interfaces in the current port group.
- Any legal IPv6 multicast MAC address except 3333-xxxx-xxxx (where x represents a hexadecimal number from 0 to F) can be manually added to the MAC address table. IPv6 multicast MAC addresses are the MAC addresses whose the least significant bit of the most significant octet is 1.

Configuration procedure

To configure an IPv6 static multicast MAC address entry in system view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure a static multicast MAC address entry.	mac-address multicast <i>mac-address interface interface-list</i> vlan <i>vlan-id</i>	No static multicast MAC address entries exist by default.

To configure an IPv6 static multicast MAC address entry in interface view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none">Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type interface-number</i>Enter port group view: port-group manual <i>port-group-name</i>	In Ethernet interface view or Layer 2 aggregate interface view, the configuration is effective on only the current interface. In port group view, the configuration is effective on all ports in the port group.
3. Configure a static multicast MAC address entry.	mac-address multicast <i>mac-address vlan vlan-id</i>	No static multicast MAC address entries exist by default.

Configuring MLD snooping port functions

Before you configure MLD snooping port functions, complete the following tasks:

- Enable MLD snooping in the VLAN.
- Configure the corresponding port groups.
- Determine the aging time of dynamic router ports.
- Determine the aging time of dynamic member ports.
- Determine the IPv6 multicast group and IPv6 multicast source addresses.

Configuring aging timers for dynamic ports

If a switch receives no MLD general queries or IPv6 PIM hello messages on a dynamic router port when the aging timer of the port expires, the switch removes the port from the router port list.

If the switch receives no MLD reports for an IPv6 multicast group on a dynamic member port when the aging timer of the port expires, the switch removes the port from the forwarding entry for the IPv6 multicast group.

If the memberships of IPv6 multicast groups change frequently, you can set a relatively small value for the aging timer of the dynamic member ports. If the memberships of IPv6 multicast groups change rarely, you can set a relatively large value.

Setting the global aging timers for dynamic ports

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD-snooping view.	mld-snooping	N/A
3. Set the global aging timer for dynamic router ports.	router-aging-time <i>interval</i>	260 seconds by default
4. Set the global aging timer for dynamic member ports.	host-aging-time <i>interval</i>	260 seconds by default

Setting the aging timers for the dynamic ports in a VLAN

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Set the aging timer for the dynamic router ports.	mld-snooping router-aging-time <i>interval</i>	260 seconds by default
4. Set the aging timer for the dynamic member ports.	mld-snooping host-aging-time <i>interval</i>	260 seconds by default

Configuring static ports

If all hosts attached to a port are interested in the IPv6 multicast data addressed to a particular IPv6 multicast group, configure the port as a static member port for that IPv6 multicast group.

You can configure a port as a static router port, through which the switch can forward all IPv6 multicast data that it received.

A static member port does not respond to queries from the MLD querier; when you configure a port as a static member port or cancel this configuration on the port, the port does not send an unsolicited MLD report or an MLD done message.

Static member ports and static router ports never age out. To remove such a port, you use the corresponding **undo** command.

To configure static ports:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
3. Configure the port as a static member port.	mld-snooping static-group <i>ipv6-group-address</i> [source-ip <i>ipv6-source-address</i>] vlan <i>vlan-id</i>	No static member ports exist by default.
4. Configure the port as a static router port.	mld-snooping static-router-port <i>vlan</i> <i>vlan-id</i>	No static router ports exist by default.

Configuring a port as a simulated member host

Generally, a host that runs MLD can respond to MLD queries. If a host fails to respond, the multicast router might deem that the IPv6 multicast group has no members on the subnet, and removes the corresponding forwarding path.

To avoid this situation, you can configure a port on the switch as a simulated member host for an IPv6 multicast group. A simulated host is equivalent to an independent host. For example, when a simulated member host receives an MLD query, it gives a response separately. Therefore, the switch can continue receiving IPv6 multicast data.

A simulated host acts like a real host in the following ways:

- When a port is configured as a simulated member host, the switch sends an unsolicited MLD report through the port, and can respond to MLD general queries with MLD reports through the port.
- When the simulated joining configuration is canceled on the port, the switch sends an MLD done message through that port.

To configure a port as a simulated member host:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.

Step	Command	Remarks
3. Configure the port as a simulated member host.	mld-snooping host-join <i>ipv6-group-address</i> [source-ip <i>ipv6-source-address</i>] vlan <i>vlan-id</i>	Not configured by default.

NOTE:

Unlike a static member port, a port that you configure as a simulated member host ages out like a dynamic member port.

Enabling fast-leave processing

The fast-leave processing feature enables the switch to process MLD done messages quickly. After the fast-leave processing feature is enabled, when the switch receives an MLD done message on a port, it immediately removes that port from the forwarding entry for the multicast group specified in the message. Then, when the switch receives MLD multicast-address-specific queries for that multicast group, it does not forward them to that port.

On a port that has only one host attached, you can enable fast-leave processing to save bandwidth and resources. However, on a port that has multiple hosts attached, you should not enable fast-leave processing if you have enabled dropping unknown IPv6 multicast data globally or for the port. Otherwise, if a host on the port leaves an IPv6 multicast group, the other hosts attached to the port in the same IPv6 multicast group cannot receive the IPv6 multicast data for the group.

Enabling fast-leave processing globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD-snooping view.	mld-snooping	N/A
3. Enable fast-leave processing.	fast-leave [vlan <i>vlan-list</i>]	Disabled by default

Enabling fast-leave processing on a port

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
3. Enable fast-leave processing.	mld-snooping fast-leave [vlan <i>vlan-list</i>]	Disabled by default.

Disabling a port from becoming a dynamic router port

The following problems exist in a multicast access network:

- After receiving an MLD general query or IPv6 PIM hello message from a connected host, a router port becomes a dynamic router port. Before its timer expires, this dynamic router port receives all multicast packets within the VLAN where the port belongs, and forwards them to the host, affecting normal multicast reception of the host.
- In addition, the MLD general query and IPv6 PIM hello message that the host sends affects the multicast routing protocol state on Layer 3 devices, such as the MLD querier or DR election, and might further cause network interruption.

To solve these problems, disable that router port from becoming a dynamic router port after the port receives an MLD general query or IPv6 PIM hello message, so as to improve network security and control over multicast users.

To disable a port from becoming a dynamic router port:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none">• Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i>• Enter port group view: port-group manual <i>port-group-name</i>	Use either command.
3. Disable the port from becoming a dynamic router port.	mld-snooping router-port-deny [vlan <i>vlan-list</i>]	By default, a port can become a dynamic router port.

NOTE:

This configuration does not affect the static router port configuration.

Configuring MLD snooping querier

Before you configure MLD snooping querier, complete the following tasks:

- Enable MLD snooping in the VLAN.
- Determine the MLD general query interval.
- Determine the MLD last-member query interval.
- Determine the maximum response time for MLD general queries.
- Determine the source IPv6 address of MLD general queries.

- Determine the source IPv6 address of MLD multicast-address-specific queries.

Enabling MLD snooping querier

In an IPv6 multicast network that runs MLD, a multicast router or Layer 3 multicast switch sends MLD queries, so that all Layer 3 multicast devices can establish and maintain multicast forwarding entries, in order to forward multicast traffic correctly at the network layer. This router or Layer 3 switch is called the "MLD querier." For more information about MLD querier, see "[Configuring MLD \(available only on the HP 5500 E1\)](#)."

However, a Layer 2 multicast switch does not support MLD. Therefore, it cannot send MLD general queries by default. When you enable MLD snooping querier on a Layer 2 switch in a VLAN where multicast traffic is switched only at Layer 2 and no Layer 3 multicast devices are present, the Layer 2 switch sends MLD queries, so that multicast forwarding entries can be created and maintained at the data link layer.

! IMPORTANT:

It is meaningless to configure an MLD snooping querier in an IPv6 multicast network that runs MLD. Although an MLD snooping querier does not participate in MLD querier elections, it might affect MLD querier elections because it sends MLD general queries with a low source IPv6 address.

To enable the MLD snooping querier:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Enable the MLD snooping querier.	mld-snooping querier	Disabled by default

Configuring parameters for MLD queries and responses

△ CAUTION:

In the configuration, make sure that the interval for sending MLD general queries is greater than the maximum response delay for MLD general queries. Otherwise, IPv6 multicast members might be deleted by mistake.

You can modify the MLD general query interval based on the actual condition of the network.

A multicast listening host starts a timer for each IPv6 multicast group that it has joined when it receives an MLD query (general query or multicast-address-specific query). This timer is initialized to a random value in the range of 0 to the maximum response delay advertised in the MLD query message. When the timer value decreases to 0, the host sends an MLD report to the IPv6 multicast group.

To speed up the response of hosts to MLD queries and avoid simultaneous timer expirations causing MLD report traffic bursts, you must properly set the maximum response delay.

- The maximum response delay for MLD general queries is set by the **max-response-time** command.
- The maximum response delay for MLD multicast-address-specific queries equals the MLD last-listener query interval.

Configuring MLD queries and responses globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD-snooping view.	mld-snooping	N/A
3. Set the maximum response delay for MLD general queries.	max-response-time <i>interval</i>	10 seconds by default
4. Set the MLD last-member query interval.	last-listener-query-interval <i>interval</i>	1 second by default

Configuring the parameters for MLD queries and responses in a VLAN

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Set the MLD query interval.	mld-snooping query-interval <i>interval</i>	125 seconds by default
4. Set the maximum response delay for MLD general queries.	mld-snooping max-response-time <i>interval</i>	10 seconds by default
5. Set the MLD last-member query interval.	mld-snooping last-listener-query-interval <i>interval</i>	1 second by default

Configuring the source IPv6 addresses for MLD queries

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Configure the source IPv6 address of MLD general queries.	mld-snooping general-query source-ip { <i>ipv6-address</i> current-interface }	FE80::02FF:FFFF:FE00:0001 by default
4. Configure the source IPv6 address of MLD multicast-address-specific queries.	mld-snooping special-query source-ip { <i>ipv6-address</i> current-interface }	FE80::02FF:FFFF:FE00:0001 by default

⚠ IMPORTANT:

The source IPv6 address of MLD query messages might affect MLD querier election within the subnet.

Configuring MLD snooping proxying

Before you configure MLD snooping proxying in a VLAN, complete the following tasks:

- Enable MLD snooping in the VLAN.
- Determine the source IPv6 address for the MLD reports sent by the proxy.
- Determine the source IPv6 address for the MLD done messages sent by the proxy.

Enabling MLD snooping proxying

The MLD snooping proxying function works on a per-VLAN basis. After you enable the function in a VLAN, the device works as the MLD snooping proxy for the downstream hosts and upstream router in the VLAN.

To enable MLD snooping proxying in a VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Enable MLD snooping proxying in the VLAN.	mld-snooping proxying enable	Disabled by default

Configuring the source IPv6 addresses for the MLD messages sent by the proxy

You can set the source IPv6 addresses for the MLD reports and done messages that the MLD snooping proxy sends on behalf of its attached hosts.

To configure the source IPv6 addresses for the MLD messages that the MLD snooping proxy sends in a VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Configure a source IPv6 address for the MLD reports that the proxy sends.	mld-snooping report source-ip { <i>ipv6-address</i> current-interface }	The default is FE80::02FF:FFFF:FE00:0001.
4. Configure a source IPv6 address for the MLD done messages that the proxy sends.	mld-snooping done source-ip { <i>ipv6-address</i> current-interface }	The default is FE80::02FF:FFFF:FE00:0001.

Configuring an MLD snooping policy

Before you configure an MLD snooping policy, complete the following tasks:

- Enable MLD snooping in the VLAN.
- Determine the IPv6 ACL rule for IPv6 multicast group filtering.
- Determine the maximum number of IPv6 multicast groups that a port can join.
- Determine the 802.1p precedence for MLD messages.

Configuring an IPv6 multicast group filter

On an MLD snooping-enabled switch, you can configure an IPv6 multicast group filter to limit multicast programs available to users.

In an application, when a user requests a multicast program, the user's host initiates an MLD report. After receiving this report message, the switch resolves the IPv6 multicast group address in the report and looks up the ACL. If a match is found to permit the port that received the report to join the IPv6 multicast group, the switch creates an MLD snooping forwarding entry for the IPv6 multicast group and adds the port to the forwarding entry. Otherwise, the switch drops this report message, in which case, the IPv6 multicast data for the IPv6 multicast group is not sent to this port, and the user cannot retrieve the program.

When you configure a multicast group filter in an IPv6 multicast VLAN, be sure to configure the filter in the sub-VLANs of the IPv6 multicast VLAN. Otherwise, the configuration does not take effect.

In an IPv6 network that runs MLDv2, when a host joins multiple multicast groups, the multicast group filter cannot correctly filter multicast groups because the host that runs MLDv2 sends multiple multicast groups that it wants to join in one membership report.

Configuring an IPv6 multicast group globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD-snooping view.	mld-snooping	N/A
3. Configure an IPv6 multicast group filter.	group-policy <i>acl6-number</i> [vlan <i>vlan-list</i>]	By default, no IPv6 group filter is globally configured. That is, the hosts in a VLAN can join any valid multicast group.

Configuring an IPv6 multicast group filter for a port

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
3. Configure an IPv6 multicast group filter.	mld-snooping group-policy <i>acl6-number</i> [vlan <i>vlan-list</i>]	By default, no IPv6 group filter is configured on an interface. That is, the hosts on the interface can join any valid multicast group.

Configuring IPv6 multicast source port filtering

When the IPv6 multicast source port filtering feature is enabled on a port, the port can connect only to IPv6 multicast receivers rather than multicast sources. The reason is that the port blocks all IPv6 multicast data packets but it permits multicast protocol packets to pass.

If this feature is disabled on a port, the port can connect to both multicast sources and IPv6 multicast receivers.

Configuring IPv6 multicast source port filtering globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD-snooping view.	mld-snooping	N/A
3. Enable IPv6 multicast source port filtering.	source-deny port <i>interface-list</i>	Disabled by default

Configuring IPv6 multicast source port filtering for a port

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view, or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
3. Enable IPv6 multicast source port filtering.	mld-snooping source-deny	Disabled by default.

NOTE:

Some models of devices, when enabled to filter IPv6 multicast data based on the source ports, are automatically enabled to filter IPv4 multicast data based on the source ports.

Enabling dropping unknown IPv6 multicast data

Unknown IPv6 multicast data refers to IPv6 multicast data for which no entries exist in the MLD snooping forwarding table. When the switch receives such IPv6 multicast traffic, one of the following occurs:

- When the function of dropping unknown IPv6 multicast data is disabled, the switch floods unknown IPv6 multicast data in the VLAN to which the unknown IPv6 multicast data belongs.
- When the function of dropping unknown IPv6 multicast data is enabled, the switch forwards unknown multicast data to its router ports instead of flooding it in the VLAN. If no router ports exist, the switch drops the unknown multicast data.

Configuration procedure

To enable dropping unknown IPv6 multicast data in a VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Enable dropping unknown IPv6 multicast data.	mld-snooping drop-unknown	Disabled by default

Configuring MLD report suppression

When a Layer 2 switch receives an MLD report from an IPv6 multicast group member, the Layer 2 switch forwards the message to the Layer 3 device that directly connects to the Layer 2 switch. When multiple members of an IPv6 multicast group are attached to the Layer 2 switch, the Layer 3 device might receive duplicate MLD reports for the IPv6 multicast group from these members.

With the MLD report suppression function enabled, within a query interval, the Layer 2 switch forwards only the first MLD report for the IPv6 multicast group to the Layer 3 device. It does not forward subsequent MLD reports for the same IPv6 multicast group to the Layer 3 device. This helps reduce the number of packets being transmitted over the network.

On an MLD snooping proxy, MLD reports for an IPv6 multicast group from downstream hosts are suppressed if the forwarding entry for the multicast group exists on the proxy, whether the suppression function is enabled or not.

To configure MLD report suppression:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter MLD-snooping view.	mld-snooping	N/A
3. Enable MLD report suppression.	report-aggregation	Enabled by default

Setting the maximum number of multicast groups that a port can join

You can set the maximum number of IPv6 multicast groups that a port can join to regulate the traffic on the port.

When you configure this maximum number, if the number of IPv6 multicast groups the port has joined exceeds the configured maximum value, the system deletes all the forwarding entries for the port from the MLD snooping forwarding table, and the hosts on this port join IPv6 multicast groups again until the number of IPv6 multicast groups that the port joins reaches the maximum value. When the port joins an IPv6 multicast group, if the port has been configured as a static member port, the system applies the configurations to the port again. If you have configured simulated joining on the port, the system establishes corresponding forwarding entry for the port after receiving a report from the simulated member host.

To configure the maximum number of IPv6 multicast groups that a port can join:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
3. Set the maximum number of IPv6 multicast groups that a port can join.	mld-snooping group-limit <i>limit</i> [vlan <i>vlan-list</i>]	1000 by default.

Enabling IPv6 multicast group replacement

For various reasons, the number of IPv6 multicast groups that a switch or a port can join might exceed the upper limit. In addition, in some specific applications, an IPv6 multicast group that the switch newly joins must replace an existing IPv6 multicast group automatically. A typical example is channel switching. To view a new TV channel, a user switches from the current IPv6 multicast group to the new one.

To realize such requirements, you can enable the IPv6 multicast group replacement function on the switch or on a certain port. When the number of IPv6 multicast groups that the switch or the port has joined reaches the limit, one of the following occurs:

- If the IPv6 multicast group replacement feature is disabled, new MLD reports are automatically discarded.
- If the IPv6 multicast group replacement feature is enabled, the IPv6 multicast group that the switch or the port newly joins automatically replaces an existing IPv6 multicast group that has the lowest IPv6 address.

! **IMPORTANT:**

Be sure to configure the maximum number of IPv6 multicast groups allowed on a port (see "[Setting the maximum number of multicast groups that a port can join](#)") before enabling IPv6 multicast group replacement. Otherwise, the IPv6 multicast group replacement functionality will not take effect.

Enabling IPv6 multicast group replacement globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD-snooping view.	mld-snooping	N/A
3. Enable IPv6 multicast group replacement.	overflow-replace [vlan <i>vlan-list</i>]	Disabled by default

Enabling IPv6 multicast group replacement for a port

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view, Layer 2 aggregate interface view, or port group view.	<ul style="list-style-type: none"> • Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type</i> <i>interface-number</i> • Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
3. Enable IPv6 multicast group replacement.	mld-snooping overflow-replace [vlan <i>vlan-list</i>]	Disabled by default.

Setting the 802.1p precedence for MLD messages

You can change the 802.1p precedence of MLD messages so that they can be assigned higher forwarding priority when congestion occurs on their outgoing ports.

Setting the 802.1p precedence for MLD messages globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD-snooping view.	mld-snooping	N/A
3. Set the 802.1p precedence for MLD messages.	dot1p-priority <i>priority-number</i>	The default 802.1p precedence for MLD messages is 0.

Setting the 802.1p precedence for MLD messages in a VLAN

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Set the 802.1p precedence for MLD messages.	mld-snooping dot1p-priority <i>priority-number</i>	The default 802.1p precedence for MLD messages is 0.

Configuring an IPv6 multicast user control policy

IPv6 multicast user control policies are configured on access switches to allow only authorized users to receive requested IPv6 multicast data. This helps restrict users from ordering certain multicast-on-demand programs.

In practice, a device first needs to perform authentication (for example, 802.1X authentication) for the connected hosts through a RADIUS server. Then, the device uses the configured multicast user control policy to perform multicast access control for authenticated users as follows.

- After receiving an MLD report from a host, the access switch matches the IPv6 multicast group address and multicast source address carried in the report with the configured policies. If a match is found, the user is allowed to join the multicast group. Otherwise, the join report is dropped by the access switch.
- After receiving a done message from a host, the access switch matches the IPv6 multicast group address and source address against the policies. If a match is found, the host is allowed to leave the group. Otherwise, the done message is dropped by the access switch.

An IPv6 multicast user control policy is functionally similar to an IPv6 multicast group filter. A difference lies in that a control policy can control both multicast joining and leaving of users based on authentication and authorization, but a multicast group filter is configured on a port to control only multicast joining but not leaving of users without authentication or authorization.

To configure a multicast user control policy

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a user profile and enter its view.	user-profile <i>profile-name</i>	N/A

Step	Command	Remarks
3. Configure a multicast user control policy.	mld-snooping access-policy <i>acl6-number</i>	No policy is configured by default. That is, a host can join or leave a valid multicast group at any time.
4. Return to system view.	quit	N/A
5. Enable the created user profile.	user-profile <i>profile-name</i> enable	Not enabled by default.

For more information about the **user-profile** and **user-profile enable** commands, see *Security Command Reference*.

Enabling the MLD snooping host tracking function

With the MLD snooping host tracking function, the switch can record the information of the member hosts that are receiving IPv6 multicast traffic, including the host IPv6 address, running duration, and timeout time. You can monitor and manage the member hosts according to the recorded information.

Enabling the MLD snooping host tracking function globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD-snooping view.	mld-snooping	N/A
3. Enable the MLD snooping host tracking function globally.	host-tracking	Disabled by default

Enabling the MLD snooping host tracking function in a VLAN

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
3. Enable the MLD snooping host tracking function in the VLAN.	mld-snooping host-tracking	Disabled by default

Setting the DSCP value for MLD messages

IPv6 uses an eight-bit Traffic class field (called ToS in IPv4) to identify type of service for IP packets. As defined in RFC 2474, the first six bits contains the DSCP priority for prioritizing traffic in the network and the last two bits are reserved.

This configuration applies to only the MLD messages that the local switch generates when the switch or its port acts as a member host, rather than those forwarded ones.

To set the DSCP value for MLD messages:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD-snooping view.	mld-snooping	N/A
3. Set the DSCP value for MLD messages.	dscp <i>dscp-value</i>	By default, the DSCP value in MLD messages is 48.

Displaying and maintaining MLD snooping

Task	Command	Remarks
Display MLD snooping group information.	display mld-snooping group [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display information about the hosts tracked by MLD snooping.	display mld-snooping host vlan <i>vlan-id</i> group <i>ipv6-group-address</i> [source <i>ipv6-source-address</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display IPv6 static multicast MAC address entries.	display mac-address [<i>mac-address</i> [vlan <i>vlan-id</i>] [multicast] [vlan <i>vlan-id</i>] [count]] [{ begin exclude include } <i>regular-expression</i>]	Available in user view.
Display statistics for the MLD messages learned through MLD snooping.	display mld-snooping statistics [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Remove dynamic group entries of a specified MLD snooping group or all MLD snooping groups.	reset mld-snooping group { <i>ipv6-group-address</i> all } [vlan <i>vlan-id</i>]	Available in user view. This command works only on an MLD snooping-enabled VLAN, but not in a VLAN with MLD enabled on its VLAN interface. This command cannot remove the static group entries of MLD snooping groups.
Clear statistics for the MLD messages learned through MLD snooping.	reset mld-snooping statistics	Available in user view.

MLD snooping configuration examples

IPv6 group policy and simulated joining configuration example

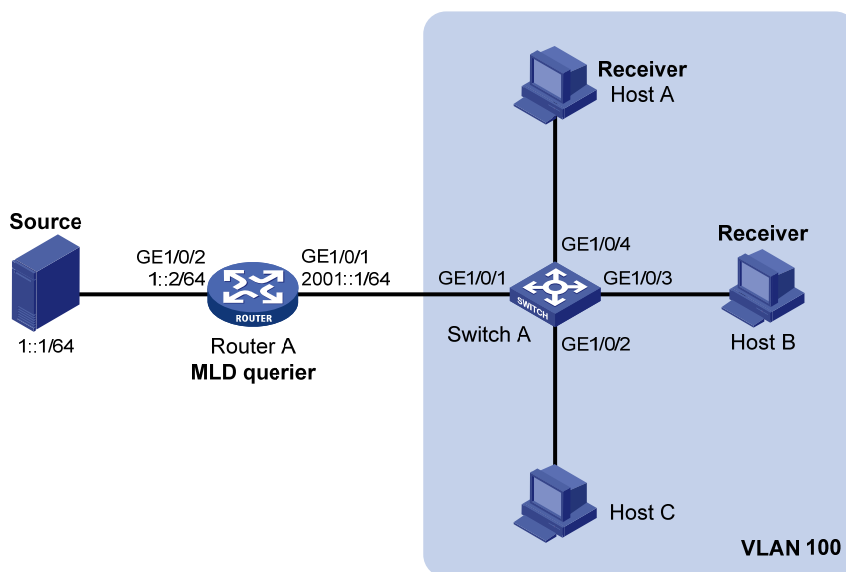
Network requirements

As shown in [Figure 70](#), MLDv1 runs on Router A, MLDv1 snooping required on Switch A, and Router A acts as the MLD querier on the subnet.

The receivers, Host A and Host B can receive IPv6 multicast traffic addressed to IPv6 multicast group FF1E::101 only.

IPv6 multicast data for group FF1E::101 can be forwarded through GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 of Switch A even if Host A and Host B accidentally, temporarily stop receiving IPv6 multicast data, and that Switch A drops unknown IPv6 multicast data and does not broadcast the data to the VLAN where Switch A resides.

Figure 70 Network diagram



Configuration procedure

1. Enable IPv6 forwarding and configure an IPv6 address and prefix length for each interface as per [Figure 70](#). (Details not shown.)
2. On Router A, Enable IPv6 multicast routing, enable IPv6 PIM-DM on each interface, and enable MLDv1 on GigabitEthernet 1/0/1.

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] pim ipv6 dm
[RouterA-GigabitEthernet1/0/1] quit
```



```
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim ipv6 dm
[RouterA-GigabitEthernet1/0/2] quit
```

3. Configure Switch A:

Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN, and enable MLD snooping and the function of dropping IPv6 unknown multicast traffic in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping drop-unknown
[SwitchA-vlan100] quit
```

Configure an IPv6 multicast group filter so that the hosts in VLAN 100 can join only the IPv6 multicast group FF1E::101.

```
[SwitchA] acl ipv6 number 2001
[SwitchA-acl6-basic-2001] rule permit source ff1e::101 128
[SwitchA-acl6-basic-2001] quit
[SwitchA] mld-snooping
[SwitchA-mld-snooping] group-policy 2001 vlan 100
[SwitchA-mld-snooping] quit
```

Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 as simulated hosts for IPv6 multicast group FF1E::101.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet1/0/4] quit
```

Verifying the configuration

Display detailed MLD snooping group information in VLAN 100 on Switch A.

```
[SwitchA] display mld-snooping group vlan 100 verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
```

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port

Subvlan flags: R-Real VLAN, C-Copy VLAN

Vlan(id):100.

```
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
```

```

Router port(s):total 1 port(s).
    GE1/0/1                (D) ( 00:01:30 )
IP group(s):the following ip group(s) match to one mac group.
IP group address:FF1E::101
  (::, FF1E::101):
  Attribute:      Host Port
  Host port(s):total 2 port(s).
    GE1/0/3                (D) ( 00:03:23 )
    GE1/0/4                (D) ( 00:04:10 )
MAC group(s):
  MAC group address:3333-0000-0101
  Host port(s):total 2 port(s).
    GE1/0/3
    GE1/0/4

```

The output shows that GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 of Switch A have joined IPv6 multicast group FF1E::101.

Static port configuration example

Network requirements

As shown in [Figure 71](#), MLDv1 runs on Router A, and MLDv1 snooping runs on Switch A, Switch B and Switch C. Router A acts as the MLD querier.

Host A and Host C are permanent receivers of IPv6 multicast group FF1E::101. GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 on Switch C are required to be configured as static member ports for multicast group FF1E::101 to enhance the reliability of multicast traffic transmission.

Suppose STP runs on the network. To avoid data loops, the forwarding path from Switch A to Switch C is blocked under normal conditions, and IPv6 multicast traffic flows to the receivers attached to Switch C only along the path of Switch A—Switch B—Switch C.

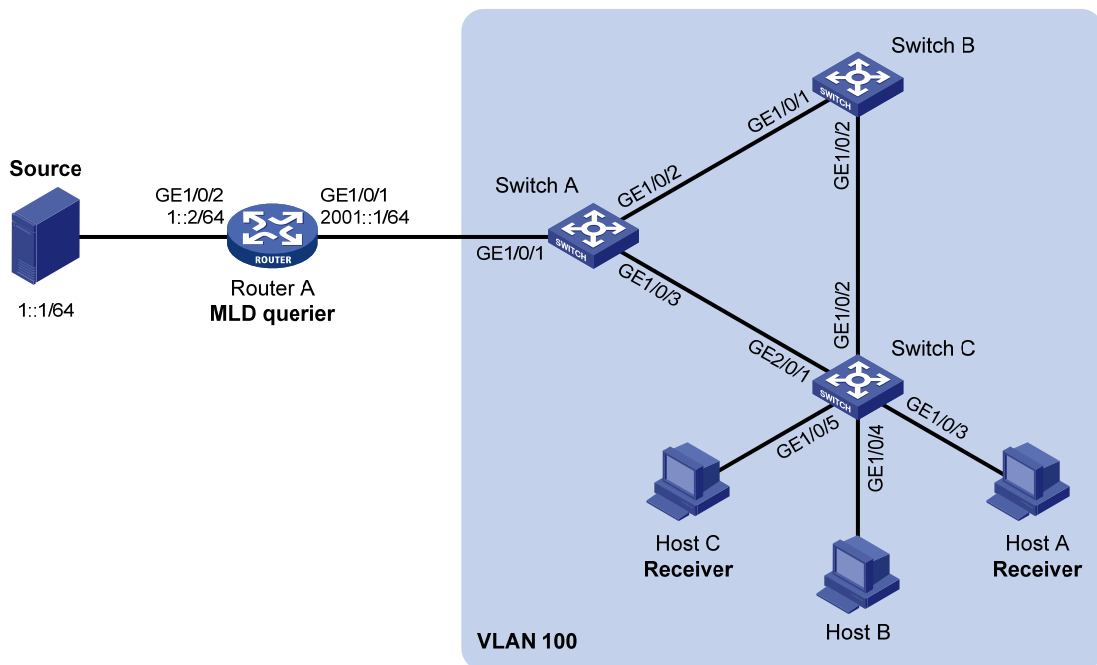
Configure GigabitEthernet 1/0/3 on Switch C as a static router port, so that IPv6 multicast traffic can flow to the receivers nearly uninterruptedly along the path of Switch A—Switch C in the case that the path of Switch A—Switch B—Switch C becomes blocked.

NOTE:

If no static router port is configured, when the path of Switch A—Switch B—Switch C becomes blocked, at least one MLD query-response cycle must be completed before the IPv6 multicast data can flow to the receivers along the new path of Switch A—Switch C. Namely, IPv6 multicast delivery will be interrupted during this process.

For more information about the Spanning Tree Protocol (STP), see *Layer 2—LAN Switching Configuration Guide*.

Figure 71 Network diagram



Configuration procedure

1. Enable IPv6 forwarding and configure an IPv6 address and prefix length for each interface as per Figure 71.
2. On Router A, enable IPv6 multicast routing, enable IPv6 PIM-DM on each interface, and enable MLD on GigabitEthernet 1/0/1.

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] pim ipv6 dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim ipv6 dm
[RouterA-GigabitEthernet1/0/2] quit
```

3. Configure Switch A:

Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to this VLAN, and enable MLD snooping in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[SwitchA-vlan100] mld-snooping enable
```

```
[SwitchA-vlan100] quit
# Configure GigabitEthernet 1/0/3 to be a static router port.
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

4. Configure Switch B:

Enable MLD snooping globally.

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

Create VLAN 100, assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to this VLAN, and enable MLD snooping in the VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] quit
```

5. Configure Switch C:

Enable MLD snooping globally.

```
<SwitchC> system-view
[SwitchC] mld-snooping
[SwitchC-mld-snooping] quit
```

Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to this VLAN, and enable MLD snooping in the VLAN.

```
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] quit
```

Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 as static member ports for IPv6 multicast group FF1E::101.

```
[SwitchC] interface GigabitEthernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
[SwitchC] interface GigabitEthernet 1/0/5
[SwitchC-GigabitEthernet1/0/5] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet1/0/5] quit
```

Verifying the configuration

Display detailed MLD snooping group information in VLAN 100 on Switch A.

```
[SwitchA] display mld-snooping group vlan 100 verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```

Vlan(id):100.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 2 port(s).
    GE1/0/1          (D) ( 00:01:30 )
    GE1/0/3          (S)
IP group(s):the following ip group(s) match to one mac group.
IP group address:FF1E::101
(::, FF1E::101):
Attribute:   Host Port
Host port(s):total 1 port(s).
    GE1/0/2          (D) ( 00:03:23 )
MAC group(s):
MAC group address:3333-0000-0101
Host port(s):total 1 port(s).
    GE1/0/2

```

The output shows that GigabitEthernet 1/0/3 of Switch A has become a static router port.

Display detailed MLD snooping group information in VLAN 100 on Switch C.

```

[SwitchC] display mld-snooping group vlan 100 verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port(s).
    GE1/0/2          (D) ( 00:01:23 )
IP group(s):the following ip group(s) match to one mac group.
IP group address:FF1E::101
(::, FF1E::101):
Attribute:   Host Port
Host port(s):total 2 port(s).
    GE1/0/3          (S)
    GE1/0/5          (S)
MAC group(s):
MAC group address:3333-0000-0101
Host port(s):total 2 port(s).
    GE1/0/3
    GE1/0/5

```

The output shows that GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 on Switch C have become static member ports for IPv6 multicast group FF1E::101.

MLD snooping querier configuration example

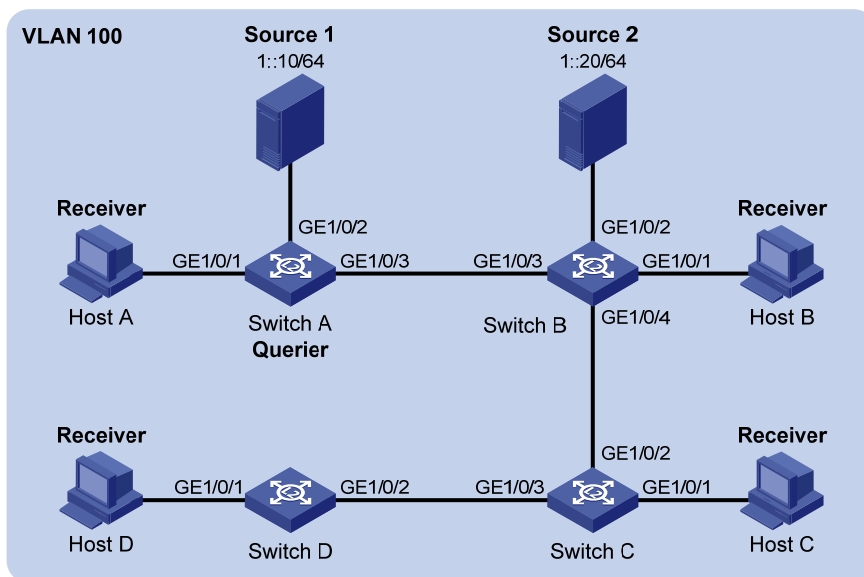
Network requirements

As shown in Figure 72, in a Layer-2-only network environment, two multicast sources (Source 1 and Source 2) send IPv6 multicast data to multicast groups FF1E::101 and FF1E::102 respectively, Host A and Host C are receivers of multicast group FF1E::101 and Host B and Host D are receivers of multicast group FF1E::102.

MLDv1 runs on all the receivers and MLDv1 snooping runs on all the switches. Switch A, which is close to the multicast sources, is chosen as the MLD snooping querier.

To prevent flooding of unknown multicast traffic within the VLAN, configure all the switches to drop unknown multicast data packets.

Figure 72 Network diagram



Configuration procedure

1. Configure Switch A:

Enable IPv6 forwarding, and enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

Create VLAN 100 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 100.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

Enable MLD snooping and the function of dropping unknown IPv6 multicast data packets in VLAN 100.

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping drop-unknown
# Configure MLD snooping querier feature in VLAN 100.
[SwitchA-vlan100] mld-snooping querier
[SwitchA-vlan100] quit
```

2. Configure Switch B:

```
# Enable IPv6 forwarding, and enable MLD snooping globally.
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit

# Create VLAN 100, add GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 into VLAN 100.
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4

# Enable the MLD snooping feature and the function of dropping unknown IPv6 multicast data packets in VLAN 100.
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] mld-snooping drop-unknown
[SwitchB-vlan100] quit
```

3. Configure Switch C and Switch D in the same way as you configure Switch B.

Verifying the configuration

When the MLD snooping querier starts to work, all the switches but the querier receive MLD general queries. Use the **display mld-snooping statistics** command to display statistics for MLD messages received.

Display the MLD message statistics on Switch B.

```
[SwitchB-vlan100] display mld-snooping statistics
Received MLD general queries:3.
Received MLDv1 specific queries:0.
Received MLDv1 reports:12.
Received MLD dones:0.
Sent MLDv1 specific queries:0.
Received MLDv2 reports:0.
Received MLDv2 reports with right and wrong records:0.
Received MLDv2 specific queries:0.
Received MLDv2 specific sg queries:0.
Sent MLDv2 specific queries:0.
Sent MLDv2 specific sg queries:0.
Received error MLD messages:0.
```

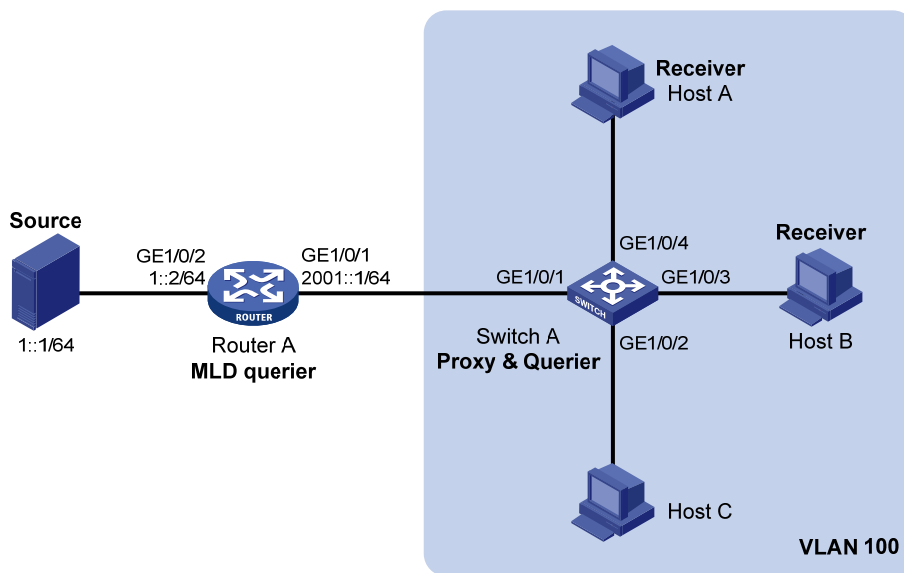
MLD snooping proxying configuration example

Network requirements

As shown in [Figure 73](#), MLDv1 runs on Router A and MLDv1 snooping runs on Switch A. Router A acts as the MLD querier.

Configure MLD snooping proxying on Switch A. This enables the switch to forward MLD reports and done messages on behalf of the attached hosts and to respond to MLD queries from Router A and then forward the queries to the hosts on behalf of Router A.

Figure 73 Network diagram



Configuration procedure

1. Configure an IP address and prefix length for each interface as per [Figure 73](#). (Details not shown.)
2. On Router A, enable IPv6 multicast routing, enable IPv6 PIM-DM on each interface, and enable MLD on port GigabitEthernet 1/0/1.

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] pim ipv6 dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim ipv6 dm
[RouterA-GigabitEthernet1/0/2] quit
```

3. Configure Switch A:

Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
```



```

[SwitchA-mld-snooping] quit
# Create VLAN 100, assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this
VLAN, and enable MLD snooping and MLD snooping proxying in the VLAN.
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping proxying enable
[SwitchA-vlan100] quit

```

Verifying the configuration

After the configuration is completed, Host A and Host B send MLD join messages addressed to group FF1E::101. When receiving the messages, Switch A sends a join message for the group out of port GigabitEthernet 1/0/1 (a router port) to Router A. Use the **display mld-snooping group** command and the **display mld group** command to display information about MLD snooping groups and MLD multicast groups. For example:

Display information about MLD snooping groups on Switch A.

```

[SwitchA] display mld-snooping group
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port(s).
    GE1/0/1                (D)
IP group(s):the following ip group(s) match to one mac group.
IP group address:FF1E::101
(::, FF1E::101):
    Host port(s):total 2 port(s).
        GE1/0/3            (D)
        GE1/0/4            (D)
MAC group(s):
    MAC group address:3333-0000-0101
    Host port(s):total 2 port(s).
        GE1/0/3
        GE1/0/4

```

Display information about MLD multicast groups on Router A.

```

[RouterA] display mld group
Total 1 MLD Group(s).
Interface group report information
GigabitEthernet1/0/1(2001::1):
Total 1 MLD Group reported

```

```
Group Address: FF1E::1
Last Reporter: FE80::2FF:FFFF:FE00:1
Uptime: 00:00:03
Expires: 00:04:17
```

When Host A leaves the IPv6 multicast group, it sends an MLD done message to Switch A. Receiving the message, Switch A removes port GigabitEthernet 1/0/4 from the member port list of the forwarding entry for the group; however, it does not remove the group or forward the done message to Router A because Host B is still in the group. Use the **display mld-snooping group** command to display information about MLD snooping groups. For example:

Display information about MLD snooping groups on Switch A.

```
[SwitchA] display mld-snooping group
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port(s).
    GE1/0/1                (D)
IP group(s):the following ip group(s) match to one mac group.
IP group address:FF1E::101
  (::, FF1E::101):
    Host port(s):total 1 port(s).
    GE1/0/3                (D)
MAC group(s):
  MAC group address:3333-0000-0101
    Host port(s):total 1 port(s).
    GE1/0/3
```

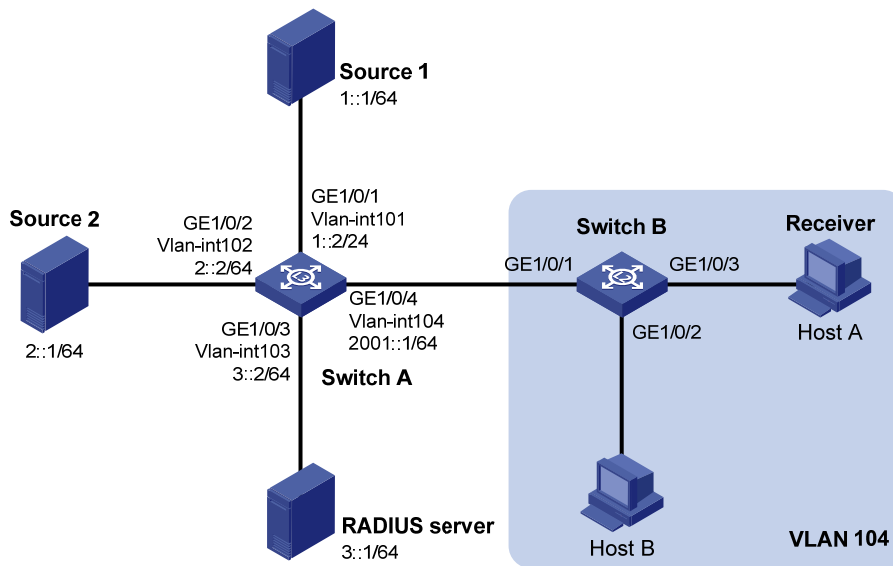
IPv6 multicast source and user control policy configuration example

Network requirements

As shown in [Figure 74](#), Switch A is a Layer-3 switch. MLDv1 runs on Switch A and MLDv1 snooping runs on Switch B. Multicast sources and hosts run 802.1X client.

An IPv6 multicast source control policy is configured on Switch A to block multicast flows from Source 2 to FF1E::101. An IPv6 multicast user control policy is configured on Switch B so that Host A can join or leave only multicast group FF1E::101.

Figure 74 Network diagram



Configuration procedures

1. Enable IPv6 forwarding and configure an IP address and prefix length for each interface as per Figure 74. (Details not shown.)
2. Configure Switch A:

Create VLAN 101 through VLAN 104 and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the four VLANs respectively.

```
<SwitchA> system-view
[SwitchA] vlan 101
[SwitchA-vlan101] port gigabitethernet 1/0/1
[SwitchA-vlan101] quit
[SwitchA] vlan 102
[SwitchA-vlan102] port gigabitethernet 1/0/2
[SwitchA-vlan102] quit
[SwitchA] vlan 103
[SwitchA-vlan103] port gigabitethernet 1/0/3
[SwitchA-vlan103] quit
[SwitchA] vlan 104
[SwitchA-vlan104] port gigabitethernet 1/0/4
[SwitchA-vlan104] quit
```

Enable IPv6 multicast routing. Enable IPv6 PIM-DM on VLAN-interface 101, VLAN-interface 102 and VLAN-interface 104, and enable MLD on VLAN-interface 104.

```
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 dm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim ipv6 dm
[SwitchA-Vlan-interface102] quit
```

```
[SwitchA] interface vlan-interface 104
[SwitchA-Vlan-interface104] pim ipv6 dm
[SwitchA-Vlan-interface104] mld enable
[SwitchA-Vlan-interface104] quit
```

Create a multicast source control policy, **policy1**, so that multicast flows from Source 2 to FF1E::101 will be blocked.

```
[SwitchA] acl ipv6 number 3001
[SwitchA-acl6-adv-3001] rule permit udp source 2::1 128 destination ffe::101 128
[SwitchA-acl6-adv-3001] quit
[SwitchA] traffic classifier classifier1
[SwitchA-classifier-classifier1] if-match acl ipv6 3001
[SwitchA-classifier-classifier1] quit
[SwitchA] traffic behavior behavior1
[SwitchA-behavior-behavior1] filter deny
[SwitchA-behavior-behavior1] quit
[SwitchA] qos policy policy1
[SwitchA-qospolicy-policy1] classifier classifier1 behavior behavior1
[SwitchA-qospolicy-policy1] quit
```

Create a user profile, apply **policy1** to the inbound direction of GE 1/0/2 in user profile view, and enable the user profile.

```
[SwitchA] user-profile profile1
[SwitchA-user-profile-profile1] qos apply policy policy1 inbound
[SwitchA-user-profile-profile1] quit
[SwitchA] user-profile profile1 enable
```

Create RADIUS scheme **scheme1**; set the service type for the RADIUS server to **extended**; specify the IP addresses of the primary authentication/authorization server and accounting server as 3::1; set the shared keys to 123321; specify that no domain name is carried in a username sent to the RADIUS server.

```
[SwitchA] radius scheme scheme1
[SwitchA-radius-scheme1] server-type extended
[SwitchA-radius-scheme1] primary authentication 3::1
[SwitchA-radius-scheme1] key authentication 123321
[SwitchA-radius-scheme1] primary accounting 3::1
[SwitchA-radius-scheme1] key accounting 123321
[SwitchA-radius-scheme1] user-name-format without-domain
[SwitchA-radius-scheme1] quit
```

Create an ISP domain **domain1**; reference **scheme1** for the authentication, authorization, and accounting for LAN users; specify **domain1** as the default ISP domain.

```
[SwitchA] domain domain1
[SwitchA-isp-domian1] authentication lan-access radius-scheme scheme1
[SwitchA-isp-domian1] authorization lan-access radius-scheme scheme1
[SwitchA-isp-domian1] accounting lan-access radius-scheme scheme1
[SwitchA-isp-domian1] quit
[SwitchA] domain default enable domain1
```

Globally enable 802.1X and then enable it on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[SwitchA] dot1x
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] dot1x
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] dot1x
[SwitchA-GigabitEthernet1/0/2] quit
```

3. Configure Switch B:

Globally enable MLD snooping.

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

Create VLAN 104, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to this VLAN, and enable MLD snooping in this VLAN.

```
[SwitchB] vlan 104
[SwitchB-vlan104] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[SwitchB-vlan104] mld-snooping enable
[SwitchB-vlan104] quit
```

Create a user profile **profile2** and configure the user profile so that users can join or leave only one IPv6 multicast group, FF1E::101. Then, enable the user profile.

```
[SwitchB] acl ipv6 number 2001
[SwitchB-acl6-basic-2001] rule permit source ff1e::101 128
[SwitchB-acl6-basic-2001] quit
[SwitchB] user-profile profile2
[SwitchB-user-profile-profile2] mld-snooping access-policy 2001
[SwitchB-user-profile-profile2] quit
[SwitchB] user-profile profile2 enable
```

Create a RADIUS scheme **scheme2**; set the service type for the RADIUS server to **extended**; specify the IP addresses of the primary authentication/authorization server and accounting server as 3::1; set the shared keys to 321123; specify that a username sent to the RADIUS server carry no domain name.

```
[SwitchB] radius scheme scheme2
[SwitchB-radius-scheme2] server-type extended
[SwitchB-radius-scheme2] primary authentication 3::1
[SwitchB-radius-scheme2] key authentication 321123
[SwitchB-radius-scheme2] primary accounting 3::1
[SwitchB-radius-scheme2] key accounting 321123
[SwitchB-radius-scheme2] user-name-format without-domain
[SwitchB-radius-scheme2] quit
```

Create an ISP domain **domain2**; reference **scheme2** for the authentication, authorization, and accounting for LAN users; specify **domain2** as the default ISP domain.

```
[SwitchB] domain domain2
[SwitchB-isp-domian2] authentication lan-access radius-scheme scheme2
[SwitchB-isp-domian2] authorization lan-access radius-scheme scheme2
[SwitchB-isp-domian2] accounting lan-access radius-scheme scheme2
```

```

[SwitchB-isp-domian2] quit
[SwitchB] domain default enable domain2
# Globally enable 802.1X and then enable it on GigabitEthernet 1/0/2 and GigabitEthernet
1/0/3.
[SwitchB] dot1x
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] dot1x
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] dot1x
[SwitchB-GigabitEthernet1/0/3] quit

```

4. Configure RADIUS server:

On the RADIUS server, configure the parameters related to Switch A and Switch B. For more information, see the configuration guide of the RADIUS server.

Verifying the configuration

After the configurations, the two multicast sources and hosts initiate 802.1X authentication. After passing the authentication, Source 1 sends multicast flows to FF1E::101 and Source 2 sends multicast flows to FF1E::102; Host A sends report messages to join IPv6 multicast groups FF1E::101 and FF1E::102. Use the **display mld-snooping group** command to display information about MLD snooping groups. For example:

Display information about MLD snooping groups in VLAN 104 on Switch B.

```

[SwitchB] display mld-snooping group vlan 104 verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):104.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port(s).
    GE1/0/1                (D) ( 00:01:30 )
IP group(s):the following ip group(s) match to one mac group.
  IP group address:FF1E::101
    (::, FF1E::101):
      Attribute:    Host Port
      Host port(s):total 1 port(s).
        GE1/0/3                (D) ( 00:04:10 )
MAC group(s):
  MAC group address:3333-0000-0101
  Host port(s):total 1 port(s).
    GE1/0/3

```

The output shows that GigabitEthernet 1/0/3 on Switch B has joined FF1E::101 but not FF1E::102.

Assume that Source 2 starts sending multicast traffic to FF1E::101. Use the **display multicast ipv6 forwarding-table** to display the IPv6 multicast forwarding table information.

Display the information about FF1E::101 in the IPv6 multicast forwarding table on Switch A.

```
[SwitchA] display multicast ipv6 forwarding-table ff1e::101
IPv6 Multicast Forwarding Table

Total 1 entry

Total 1 entry matched
00001. (1::1, FF1E::101)
  MID: 0, Flags: 0x0:0
  Uptime: 00:08:32, Timeout in: 00:03:26
  Incoming interface: Vlan-interface101
  List of 1 outgoing interfaces:
    1: Vlan-interface104
  Matched 19648 packets(20512512 bytes), Wrong If 0 packets
  Forwarded 19648 packets(20512512 bytes)
```

The output shows that Switch A maintains a multicast forwarding entry for multicast packets from Source 1 to FF1E::101. No forwarding entry exists for packets from Source 2 to FF1E::101, which indicates that IPv6 multicast packets from Source 2 are blocked.

Troubleshooting MLD snooping

Layer 2 multicast forwarding cannot function

Symptom

Layer 2 multicast forwarding cannot function.

Analysis

MLD snooping is not enabled.

Solution

1. Use the **display current-configuration** command to display the running status of MLD snooping.
2. If MLD snooping is not enabled, use the **mld-snooping** command to enable MLD snooping globally, and then use **mld-snooping enable** command to enable MLD snooping in VLAN view.
3. If MLD snooping is disabled only for the corresponding VLAN, use the **mld-snooping enable** command in VLAN view to enable MLD snooping in the corresponding VLAN.

Configured IPv6 multicast group policy fails to take effect

Symptom

Although an IPv6 multicast group policy has been configured to allow hosts to join specific IPv6 multicast groups, the hosts can still receive IPv6 multicast data addressed to other groups.

Analysis

- The IPv6 ACL rule is incorrectly configured.
- The IPv6 multicast group policy is not correctly applied.
- The function of dropping unknown IPv6 multicast data is not enabled, so unknown IPv6 multicast data is flooded.

Solution

1. Use the **display acl ipv6** command to check the configured IPv6 ACL rule. Make sure that the IPv6 ACL rule conforms to the IPv6 multicast group policy to be implemented.
2. Use the **display this** command in MLD-snooping view or the corresponding interface view to verify that the correct IPv6 multicast group policy has been applied. If not, use the **group-policy** or **mld-snooping group-policy** command to apply the correct IPv6 multicast group policy.
3. Use the **display current-configuration** command to verify that the function of dropping unknown IPv6 multicast data is enabled. If not, use the **mld-snooping drop-unknown** command to enable the function of dropping unknown IPv6 multicast data.

Appendix

Processing of IPv6 multicast protocol messages

With Layer 3 multicast routing enabled, an MLD snooping-enabled switch processes IPv6 multicast protocol messages differently under different conditions, as follows:

1. If only MLD is enabled on the switch, or if both MLD and IPv6 PIM are enabled on the switch, the switch does the following:
 - Maintains dynamic member ports or dynamic router ports according to MLD packets
 - Maintains dynamic router ports according to IPv6 PIM hello packets
2. If only IPv6 PIM is enabled on the switch, the following occurs:
 - The switch broadcasts MLD messages as unknown messages in the VLAN.
 - After receiving an IPv6 PIM hello message, the switch maintains the corresponding dynamic router port.
3. If MLD is disabled on the switch, one of the following occurs:
 - If IPv6 PIM is disabled, the switch deletes all its dynamic member ports and dynamic router ports.

- If IPv6 PIM is enabled, the switch deletes only its dynamic member ports but not its dynamic router ports.

NOTE:

On a switch with Layer-3 IPv6 multicast routing enabled, use the **display mld group port-info** command to display Layer-2 port information.

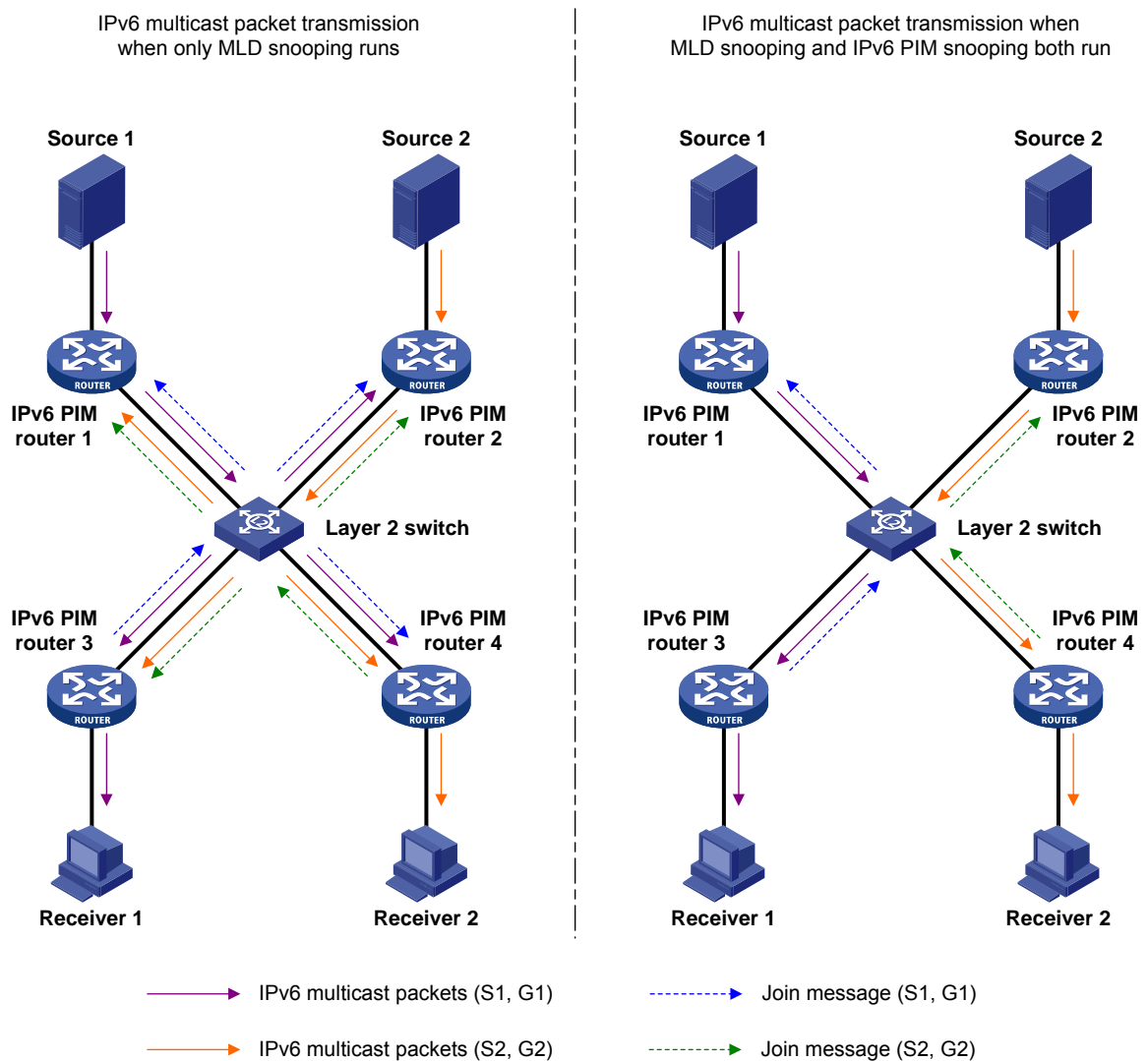
4. If IPv6 PIM is disabled on the switch, one of the following occurs:
 - If MLD is disabled, the switch deletes all its dynamic router ports.
 - If MLD is enabled, the switch maintains all its dynamic member ports and dynamic router ports.

Configuring IPv6 PIM snooping

Overview

IPv6 Protocol Independent Multicast (PIM) snooping runs on Layer 2 devices. It determines which ports are interested in multicast data by analyzing the received IPv6 PIM messages, and adds the ports to a multicast forwarding entry to make sure that multicast data can be forwarded to only the ports that are interested in the data.

Figure 75 Multicast packet transmission without or with IPv6 PIM snooping



As shown in Figure 75, Source 1 sends multicast data to multicast group G1, and Source 2 sends multicast data to multicast group G2. Receiver 1 belongs to G1, and Receiver 2 belongs to G2. The Layer 2 switch's interfaces that connect to the IPv6 PIM-capable routers are in the same VLAN.

- When running MLD snooping without IPv6 PIM snooping, the Layer 2 switch maintains the router ports according to IPv6 PIM hello messages received from IPv6 PIM-capable routers, broadcasts all other types of received IPv6 PIM messages in the VLAN, and forwards all multicast data to all router ports in the VLAN. Each IPv6 PIM-capable router in the VLAN, whether interested in the multicast data or not, will receive all multicast data and all IPv6 PIM messages except for IPv6 PIM hello messages.
- If the Layer 2 switch runs both MLD snooping and IPv6 PIM snooping, it determines whether an IPv6 PIM-capable router is interested in the multicast data destined for a multicast group according to the received IPv6 PIM messages that the router sends, and adds the port that connects to the router to a multicast forwarding entry. Then, the Layer 2 switch can correctly forward IPv6 PIM messages and the multicast data only to the router according to the multicast forwarding entry, saving network bandwidth.

For more information about MLD snooping and the router port, see "[Configuring MLD snooping](#)."

For more information about IPv6 PIM, see "[Configuring IPv6 PIM \(available only on the HP 5500 EI\)](#)."

Configuring IPv6 PIM snooping

When you configure IPv6 PIM snooping, follow these guidelines:

- Before you configure IPv6 PIM snooping for a VLAN, you must enable IPv6 forwarding and MLD snooping globally and enable MLD snooping in the VLAN.
- IPv6 PIM snooping does not work in the sub-VLANs of a multicast VLAN. For more information about IPv6 multicast VLAN, see "[Configuring IPv6 multicast VLANs](#)."
- In a network with IPv6 PIM snooping enabled switches, configure the size of each join/prune message no more than the path maximum transmission unit (MTU) on the IPv6 PIM-enabled edge router on the receiver side. For more information about the join/prune messages, see "[Configuring IPv6 PIM \(available only on the HP 5500 EI\)](#)."
- After you enable IPv6 PIM snooping in a VLAN, IPv6 PIM snooping works only on the member interfaces of the VLAN.

To configure IPv6 PIM snooping:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IPv6 forwarding globally.	ipv6	Disabled by default
3. Enable MLD snooping globally and enter MLD-snooping view.	mld-snooping	Disabled by default
4. Return to system view.	quit	N/A
5. Enter VLAN view.	vlan <i>vlan-id</i>	N/A
6. Enable MLD snooping in the VLAN.	mld-snooping enable	Disabled by default

Step	Command	Remarks
7. Enable IPv6 PIM snooping in the VLAN.	pim-snooping ipv6 enable	Disabled by default

Displaying and maintaining IPv6 PIM snooping

Task	Command	Remarks
Display IPv6 PIM snooping neighbor information.	display pim-snooping ipv6 neighbor [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv6 PIM snooping routing entries.	display pim-snooping ipv6 routing-table [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the statistics information of IPv6 PIM messages learned by IPv6 PIM snooping.	display pim-snooping ipv6 statistics [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Clear the statistics information of IPv6 PIM messages learned by IPv6 PIM snooping.	reset pim-snooping ipv6 statistics	Available in user view

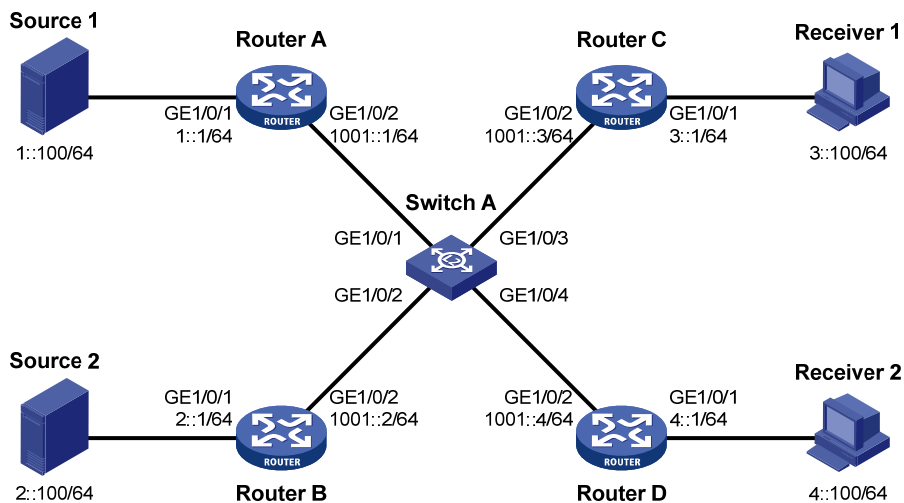
IPv6 PIM snooping configuration example

Network requirements

As shown in [Figure 76](#), Source 1 sends multicast data to IPv6 multicast group FF1E::101, and Source 2 sends multicast data to IPv6 multicast group FF2E::101. Receiver 1 belongs to multicast group FF1E::101, and Receiver 2 belongs to multicast group FF2E::101. Router C and Router D run MLD on their interface GigabitEthernet 1/0/1. Router A, Router B, Router C, and Router D run IPv6 PIM-SM, and interface GigabitEthernet 1/0/2 on Router A acts as a C-BSR and C-RP.

Configure MLD snooping and IPv6 PIM snooping on Switch A so that Switch A forwards IPv6 PIM messages and multicast data to only the routers that are interested in the multicast data.

Figure 76 Network diagram



Configuration procedure

1. Enable IPv6 forwarding on the devices, configure an IPv6 address and prefix length for each interface according to Figure 76. (Details not shown.)
2. On Router A, enable IPv6 multicast routing, enable IPv6 PIM-SM on each interface, and configure interface GigabitEthernet 1/0/2 as a C-BSR and C-RP.

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim ipv6 sm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim ipv6 sm
[RouterA-GigabitEthernet1/0/2] quit
[RouterA] pim ipv6
[RouterA-pim6] c-bsr 1001::1
[RouterA-pim6] c-rp 1001::1
```

3. On Router B, enable IPv6 multicast routing, and enable IPv6 PIM-SM on each interface.

```
<RouterB> system-view
[RouterB] multicast ipv6 routing-enable
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] pim ipv6 sm
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] pim ipv6 sm
```

4. On Router C, enable IPv6 multicast routing, enable IPv6 PIM-SM on each interface, and enable MLD on GigabitEthernet 1/0/1.

```
<RouterC> system-view
[RouterC] multicast ipv6 routing-enable
[RouterC] interface gigabitethernet 1/0/1
```

```
[RouterC-GigabitEthernet1/0/1] pim ipv6 sm
[RouterC-GigabitEthernet1/0/1] mld enable
[RouterC-GigabitEthernet1/0/1] quit
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] pim ipv6 sm
```

5. Configure Router D in the same way as you configure Router C. (Details not shown.)

6. Configure Switch A:

Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

Create VLAN 100, assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to this VLAN, and enable MLD snooping and IPv6 PIM snooping in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] pim-snooping ipv6 enable
[SwitchA-vlan100] quit
```

Verifying the configuration

On Switch A, display the IPv6 PIM snooping neighbor information of VLAN 100.

```
[SwitchA] display pim-snooping ipv6 neighbor vlan 100
Total number of neighbors: 4
```

```
VLAN ID: 100
```

```
Total number of neighbors: 4
```

Neighbor	Port	Expires	Option Flags
FE80::1	GE1/0/1	02:02:23	LAN Prune Delay
FE80::2	GE1/0/2	03:00:05	LAN Prune Delay
FE80::3	GE1/0/3	02:22:13	LAN Prune Delay
FE80::4	GE1/0/4	03:07:22	LAN Prune Delay

The output shows that Router A, Router B, Router C, and Router D are IPv6 PIM snooping neighbors.

On Switch A, display the IPv6 PIM snooping routing information of VLAN 100.

```
[SwitchA] display pim-snooping ipv6 routing-table vlan 100 slot 1
Total 2 entry(ies)
FSM Flag: NI-no info, J-join, PP-prune pending
```

```
VLAN ID: 100
```

```
Total 2 entry(ies)
```

```
(*, FF1E::101)
```

```
Upstream neighbor: FE80::1
```

```
Upstream port: GE1/0/1
```

```
Total number of downstream ports: 1
```

```
1: GE1/0/3
```

```
Expires: 00:03:01, FSM: J
```

```
(*, FF2E::101)
```

```
Upstream neighbor: FE80::2
Upstream port: GE1/0/2
Total number of downstream ports: 1
  1: GE1/0/4
Expires: 00:01:05, FSM: J
```

The output shows that Switch A will forward the multicast data intended for IPv6 multicast group FF1E::101 to only Router C, and forward the multicast data intended for IPv6 multicast group FF2E::101 to only Router D.

Troubleshooting IPv6 PIM snooping

IPv6 PIM snooping does not work

Symptom

IPv6 PIM snooping does not work.

Analysis

MLD snooping or IPv6 PIM snooping is not enabled on the switch.

Solution

1. Use the **display current-configuration** command to check the status of MLD snooping and IPv6 PIM snooping.
2. If MLD snooping is not enabled, enter system view and use the **mld-snooping** command to enable MLD snooping globally. Then, enter VLAN view and use the **mld-snooping enable** and **pim-snooping ipv6 enable** commands to enable MLD snooping and IPv6 PIM snooping in the VLAN.
3. If IPv6 PIM snooping is not enabled, enter VLAN view and use the **pim-snooping ipv6 enable** command to enable IPv6 PIM snooping in the VLAN.

Some downstream IPv6 PIM-capable routers cannot receive multicast data

Symptom

In a network with fragmented join/prune messages, some downstream IPv6 PIM-capable routers cannot receive multicast data.

Analysis

IPv6 PIM snooping cannot reassemble messages, and it cannot maintain the status of downstream routers that the join/prune message fragments carry. To ensure the normal operation of the system, IPv6 PIM snooping must broadcast join/prune message fragments in the VLAN. However, if the VLAN has an IPv6 PIM-capable router that has the join suppression function enabled, the broadcast join/prune

message fragments might suppress the join messages of other IPv6 PIM-capable routers in the VLAN. As a result, some IPv6 PIM-capable routers cannot receive the multicast data addressed to a specific multicast group because their join messages are suppressed. To solve this problem, disable the join suppression function on all IPv6 PIM-capable routers that connect to the IPv6 PIM snooping-capable switch in the VLAN.

Solution

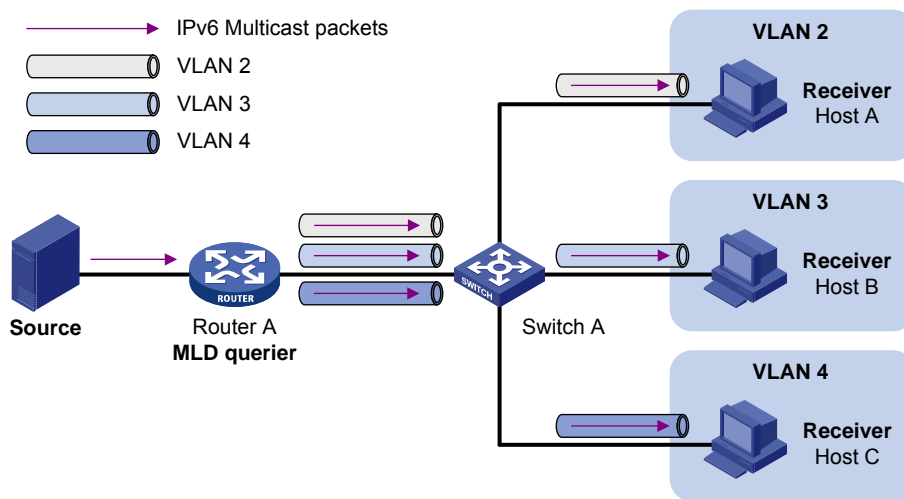
1. Use the **pim ipv6 hello-option neighbor-tracking** command to enable the neighbor tracking function on the interfaces of IPv6 PIM-capable routers that connect to the IPv6 PIM snooping-capable switch.
2. If the network has an IPv6 PIM-capable router that cannot be enabled with the neighbor tracking function, be sure to disable IPv6 PIM snooping on the IPv6 PIM snooping-capable switch.

Configuring IPv6 multicast VLANs

Overview

As shown in [Figure 77](#), in the traditional IPv6 multicast programs-on-demand mode, when hosts (Host A, Host B, and Host C), which belong to different VLANs, require IPv6 multicast programs on demand service, the Layer 3 device, Router A, must forward a separate copy of the multicast traffic in each user VLAN to the Layer 2 device, Switch A. This results in not only waste of network bandwidth but also extra burden on the Layer 3 device.

Figure 77 Multicast transmission without IPv6 multicast VLAN



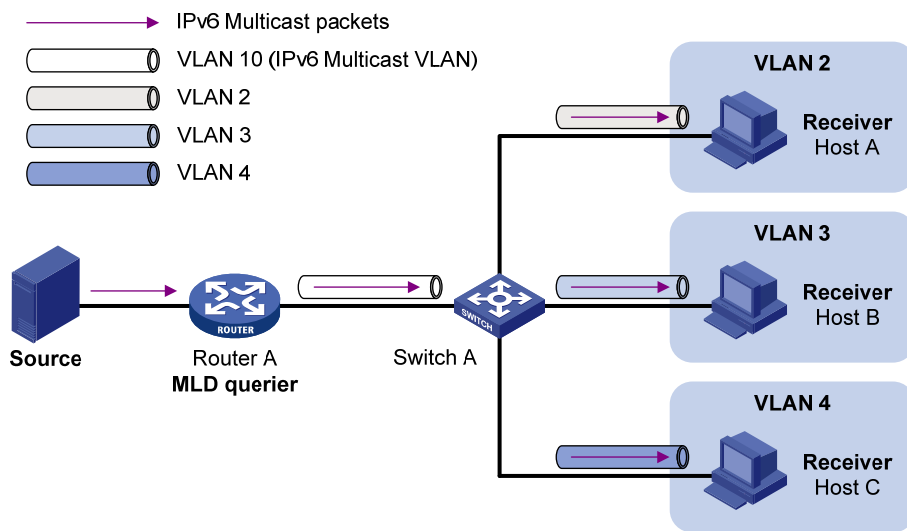
The IPv6 multicast VLAN feature configured on the Layer 2 device is the solution to this issue. With the IPv6 multicast VLAN feature, the Layer 3 device needs to replicate the multicast traffic only in the IPv6 multicast VLAN instead of making a separate copy of the multicast traffic in each user VLAN. This saves the network bandwidth and lessens the burden of the Layer 3 device.

The IPv6 multicast VLAN feature can be implemented in sub-VLAN-based IPv6 multicast VLAN and port-based IPv6 multicast VLAN.

Sub-VLAN-based IPv6 multicast VLAN

As shown in [Figure 78](#), Host A, Host B and Host C are in different user VLANs. On Switch A, configure VLAN 10 as an IPv6 multicast VLAN, configure all the user VLANs as sub-VLANs of VLAN 10, and enable MLD snooping in the IPv6 multicast VLAN.

Figure 78 Sub-VLAN-based IPv6 multicast VLAN

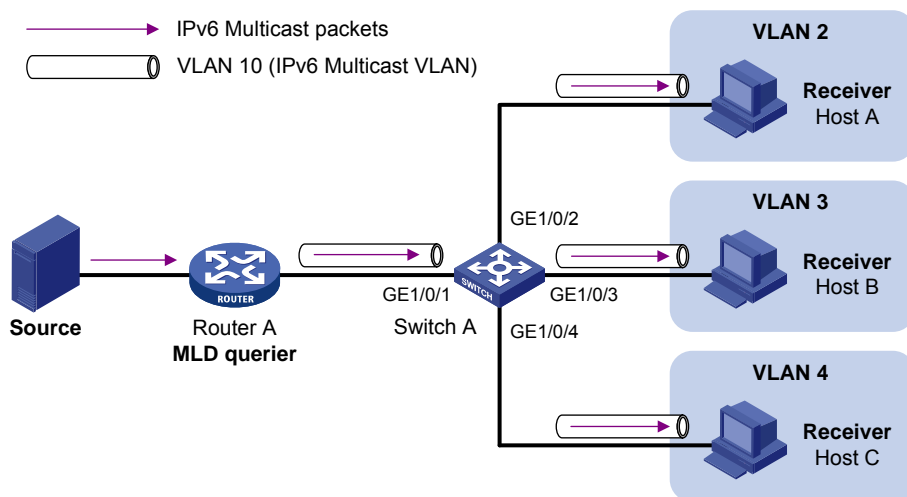


After the configuration, MLD snooping manages router ports in the IPv6 multicast VLAN and member ports in the sub-VLANs. When forwarding multicast data to Switch A, Router A sends only one copy of multicast data to Switch A in the IPv6 multicast VLAN, and Switch A distributes the data to the sub-VLANs that contain receivers.

Port-based IPv6 multicast VLAN

As shown in Figure 79, Host A, Host B, and Host C are in different user VLANs. All the user ports are hybrid ports. On Switch A, configure VLAN 10 as an IPv6 multicast VLAN, assign all the user ports to VLAN 10, and enable MLD snooping in the IPv6 multicast VLAN and all user VLANs.

Figure 79 Port-based IPv6 multicast VLAN



After the configuration, if Switch A receives an MLD message on a user port, it tags the message with the IPv6 multicast VLAN ID and relays it to the MLD querier, so that MLD snooping can uniformly manage the router ports and member ports in the IPv6 multicast VLAN. When Router A forwards multicast data to

Switch A, it sends only one copy of multicast data to Switch A in the IPv6 multicast VLAN, and Switch A distributes the data to all member ports in the IPv6 multicast VLAN.

For more information about MLD snooping, router ports, and member ports, see "[Configuring MLD snooping](#)."

For more information about VLAN tags, see *Layer 2—LAN Switching Configuration Guide*.

IPv6 multicast VLAN configuration task list

Configuration task	Remarks
Configuring a sub-VLAN-based IPv6 multicast VLAN	Required.
Configuring a port-based IPv6 multicast VLAN	Configuring user port attributes
	Configuring IPv6 multicast VLAN ports

NOTE:

If you have configured both sub-VLAN-based IPv6 multicast VLAN and port-based IPv6 multicast VLAN on a device, the port-based IPv6 multicast VLAN configuration is given preference.

Configuring a sub-VLAN-based IPv6 multicast VLAN

Before you configure a sub-VLAN-based IPv6 multicast VLAN, complete the following tasks:

- Enable IPv6 forwarding.
- Create VLANs as required.
- Enable MLD snooping in the VLAN to be configured as an IPv6 multicast VLAN.

Configuration guidelines

- For the HP 5500 EI switches, you cannot configure an IPv6 multicast VLAN on a device with IP multicast routing enabled.
- The VLAN to be configured as an IPv6 multicast VLAN must exist.
- The VLANs to be configured as the sub-VLANs of the IPv6 multicast VLAN must exist and must not be IPv6 multicast VLANs or sub-VLANs of any other IPv6 multicast VLAN.
- The total number of sub-VLANs of an IPv6 multicast VLAN must not exceed the maximum number the system can support.

Configuration procedure

In this approach, you configure a VLAN as an IPv6 multicast VLAN, and configure user VLANs as sub-VLANs of the IPv6 multicast VLAN.

To configure a sub-VLAN-based IPv6 multicast VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.	multicast-vlan ipv6 <i>vlan-id</i>	No IPv6 multicast VLAN configured by default.
3. Configure the specified VLANs as sub-VLANs of the IPv6 multicast VLAN.	subvlan <i>vlan-list</i>	By default, an IPv6 multicast VLAN has no sub-VLANs.

Configuring a port-based IPv6 multicast VLAN

When you configure a port-based IPv6 multicast VLAN, you need to configure the attributes of each user port and then assign the ports to the IPv6 multicast VLAN.

A user port can be configured as a multicast VLAN port only if it is an Ethernet port or Layer 2 aggregate interface.

In Ethernet interface view or Layer 2 aggregate interface view, configurations that you make are effective only on the current interface. In port group view, configurations that you make are effective on all ports in the current port group.

Configuration prerequisites

Before you configure a port-based IPv6 multicast VLAN, complete the following tasks:

- Enable IPv6 forwarding.
- Create VLANs as required.
- Enable MLD snooping in the VLAN to be configured as an IPv6 multicast VLAN.
- Enable MLD snooping in all the user VLANs.

Configuring user port attributes

First, configure the user ports as hybrid ports to permit packets of the specified user VLAN to pass and configure the user VLAN to which the user ports belong as the default VLAN.

Then, configure the user ports to permit packets of the IPv6 multicast VLAN to pass and untag the packets. After receiving multicast packets tagged with the IPv6 multicast VLAN ID from the upstream device, the Layer 2 device untags the multicast packets and forwards them to its downstream device.

To configure user port attributes:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
3. Configure the user port link type as hybrid.	port link-type hybrid	Access by default.
4. Specify the user VLAN that comprises the current user ports as the default VLAN.	port hybrid pvid vlan <i>vlan-id</i>	VLAN 1 by default.
5. Configure the current user ports to permit packets of the specified IPv6 multicast VLAN to pass and untag the packets.	port hybrid vlan <i>vlan-id-list</i> { tagged untagged }	By default, a hybrid port permits only packets of VLAN 1 to pass.

For more information about the **port link-type**, **port hybrid pvid vlan**, and **port hybrid vlan** commands, see *Layer 2—LAN Switching Command Reference*.

Configuring IPv6 multicast VLAN ports

In this approach, you configure a VLAN as an IPv6 multicast VLAN and assign user ports to it. You can do this by either adding the user ports in the IPv6 multicast VLAN or specifying the IPv6 multicast VLAN on the user ports. These two methods provide the same result.

Configuration guidelines

- For the HP 5500 EI switches, you cannot configure an IPv6 multicast VLAN on a device with multicast routing enabled.
- The VLAN to be configured as an IPv6 multicast VLAN must exist.
- A port can belong to only one IPv6 multicast VLAN.

Configuration procedure

To configure IPv6 multicast VLAN ports in IPv6 multicast VLAN view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.	multicast-vlan ipv6 <i>vlan-id</i>	No IPv6 multicast VLAN configured by default.

Step	Command	Remarks
3. Configure the ports as member ports of the IPv6 multicast VLAN.	port <i>interface-list</i>	By default, an IPv6 multicast VLAN has no member ports.

To configure IPv6 multicast VLAN ports in interface view or port group view:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.	multicast-vlan ipv6 <i>vlan-id</i>	Not an IPv6 multicast VLAN by default.
3. Return to system view.	quit	N/A
4. Enter interface view or port group view.	<ul style="list-style-type: none"> Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view: interface <i>interface-type interface-number</i> Enter port group view: port-group manual <i>port-group-name</i> 	Use either command.
5. Configure the ports as member ports of the IPv6 multicast VLAN.	port multicast-vlan ipv6 <i>vlan-id</i>	By default, a user port does not belong to any IPv6 multicast VLAN.

Displaying and maintaining IPv6 multicast VLAN

Task	Command	Remarks
Display information about an IPv6 multicast VLAN.	display multicast-vlan ipv6 [<i>vlan-id</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view

IPv6 multicast VLAN configuration examples

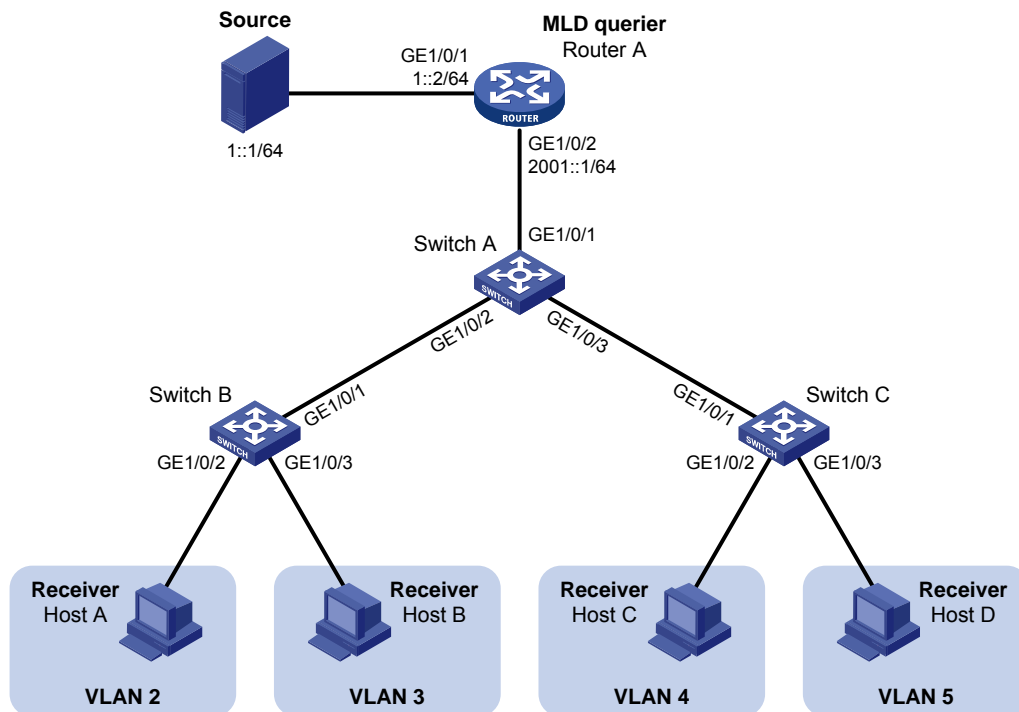
Sub-VLAN-based multicast VLAN configuration example

Network requirements

As shown in [Figure 80](#), MLDv1 runs on Router A, and MLDv1 snooping runs on Switch A. Router A acts as the MLD querier. The IPv6 multicast source sends IPv6 multicast data to the IPv6 multicast group FF1E::101. Host A, Host B, Host C, and Host D are receivers of the IPv6 multicast group. The hosts belong to VLAN 2 through VLAN 5 respectively.

Configure the sub-VLAN-based IPv6 multicast VLAN feature on Switch A so that Router A just sends IPv6 multicast data to Switch A through the IPv6 multicast VLAN and Switch A forwards the traffic to the receivers that belong to different user VLANs.

Figure 80 Network diagram



Configuration procedure

1. Enable IPv6 forwarding on each device and configure an IPv6 address and address prefix for each interface as per Figure 80. (Details not shown.)
2. On Router A, enable IPv6 multicast routing, enable IPv6 PIM-DM on each interface and enable MLD on the host-side interface GigabitEthernet 1/0/2.

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim ipv6 dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim ipv6 dm
[RouterA-GigabitEthernet1/0/2] mld enable
```

3. Configure Switch A:

Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

Create VLAN 2 through VLAN 5.

```
[SwitchA] vlan 2 to 5
```

Configure GigabitEthernet 1/0/2 as a trunk port that permits packets from VLAN 2 and VLAN 3 to pass through.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 2 3
[SwitchA-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a trunk port that permits packets from VLAN 4 and VLAN 5 to pass through.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 4 5
[SwitchA-GigabitEthernet1/0/3] quit
```

Create VLAN 10, assign GigabitEthernet 1/0/1 to this VLAN and enable MLD snooping in the VLAN.

```
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] mld-snooping enable
[SwitchA-vlan10] quit
```

Configure VLAN 10 as an IPv6 multicast VLAN and configure VLAN 2 through VLAN 5 as its sub-VLANs.

```
[SwitchA] multicast-vlan ipv6 10
[SwitchA-ipv6-mvlan-10] subvlan 2 to 5
[SwitchA-ipv6-mvlan-10] quit
```

4. Configure Switch B:

Enable MLD snooping globally.

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

Create VLAN 2, assign GigabitEthernet 1/0/2 to VLAN 2, and enable MLD snooping in the VLAN.

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/2
[SwitchB-vlan2] mld-snooping enable
[SwitchB-vlan2] quit
```

Create VLAN 3, assign GigabitEthernet 1/0/3 to VLAN 3, and enable MLD snooping in the VLAN.

```
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3
[SwitchB-vlan3] mld-snooping enable
[SwitchB-vlan3] quit
```

Configure GigabitEthernet 1/0/1 as a trunk port that permits packets from VLAN 2 and VLAN 3 to pass through.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2 3
```

5. Configure Switch C in the same way as you configure Switch B. (Details not shown.)

Verifying the configuration

Display information about the IPv6 multicast VLAN.

```
[SwitchA] display multicast-vlan ipv6
Total 1 IPv6 multicast-vlan(s)
IPv6 Multicast vlan 10
  subvlan list:
    vlan 2-5
  port list:
    no port
```

Display the MLD snooping IPv6 multicast group information on Switch A.

```
[SwitchA] display mld-snooping group
Total 5 IP Group(s).
Total 5 IP Source(s).
Total 5 MAC Group(s).
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):2.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 0 port(s).
  IP group(s):the following ip group(s) match to one mac group.
    IP group address:FF1E::101
      (::, FF1E::101):
        Host port(s):total 1 port(s).
          GE1/0/2          (D)
  MAC group(s):
    MAC group address:3333-0000-0101
      Host port(s):total 1 port(s).
        GE1/0/2
Vlan(id):3.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 0 port(s).
  IP group(s):the following ip group(s) match to one mac group.
    IP group address:FF1E::101
      (::, FF1E::101):
        Host port(s):total 1 port(s).
          GE1/0/2          (D)
  MAC group(s):
    MAC group address:3333-0000-0101
      Host port(s):total 1 port(s).
        GE1/0/2
Vlan(id):4.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
Router port(s):total 0 port(s).
IP group(s):the following ip group(s) match to one mac group.
  IP group address:FF1E::101
    (::, FF1E::101):
      Host port(s):total 1 port(s).
        GE1/0/3                (D)
MAC group(s):
  MAC group address:3333-0000-0101
    Host port(s):total 1 port(s).
      GE1/0/3
```

Vlan(id):5.

```
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 0 port(s).
IP group(s):the following ip group(s) match to one mac group.
  IP group address:FF1E::101
    (::, FF1E::101):
      Host port(s):total 1 port(s).
        GE1/0/3                (D)
MAC group(s):
  MAC group address:3333-0000-0101
    Host port(s):total 1 port(s).
      GE1/0/3
```

Vlan(id):10.

```
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port(s).
      GE1/0/1                (D)
IP group(s):the following ip group(s) match to one mac group.
  IP group address:FF1E::101
    (::, FF1E::101):
      Host port(s):total 0 port(s).
MAC group(s):
  MAC group address:3333-0000-0101
    Host port(s):total 0 port(s).
```

The output shows that MLD snooping is maintaining the router port in the IPv6 multicast VLAN (VLAN 10) and the member ports in the sub-VLANs (VLAN 2 through VLAN 5).

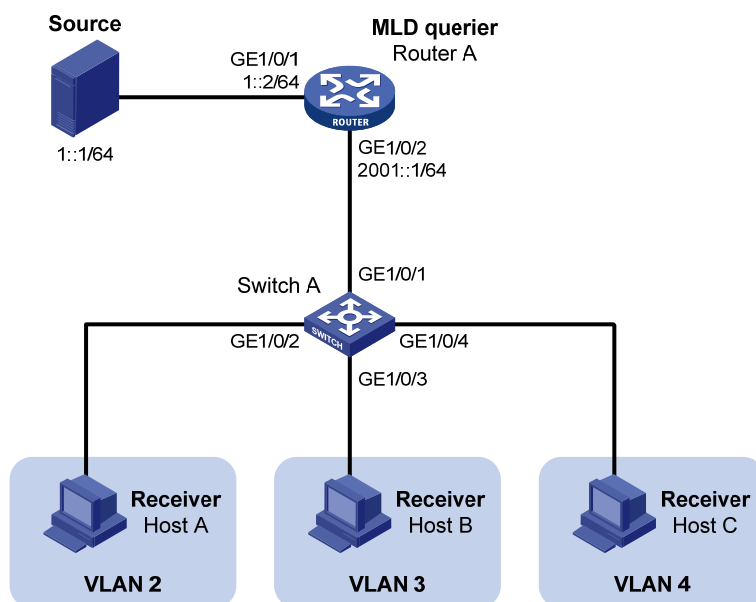
Port-based multicast VLAN configuration example

Network requirements

As shown in [Figure 81](#), MLDv1 runs on Router A. MLDv1 snooping runs on Switch A. Router A acts as the MLD querier. The IPv6 multicast source sends IPv6 multicast data to IPv6 multicast group FF1E::101. Host A, Host B, and Host C are receivers of the IPv6 multicast group. The hosts belong to VLAN 2 through VLAN 4 respectively.

Configure the port-based IPv6 multicast VLAN feature on Switch A so that Router A sends IPv6 multicast data to Switch A through the IPv6 multicast VLAN, and Switch A forwards the IPv6 multicast data to the receivers that belong to different user VLANs.

Figure 81 Network diagram



Configuration procedure

1. Enable IPv6 forwarding on each device, and configure the IPv6 address and address prefix for each interface as per [Figure 81](#). (Details not shown.)
2. On Router A, enable IPv6 multicast routing, enable IPv6 PIM-DM on each interface, and enable MLD on the host-side interface GigabitEthernet 1/0/2.

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ipv6 pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ipv6 pim dm
[RouterA-GigabitEthernet1/0/2] mld enable
```

3. Configure Switch A:

Enable MLD snooping globally.

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

Create VLAN 10, assign GigabitEthernet 1/0/1 to VLAN 10, and enable MLD snooping in this VLAN.

```
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] mld-snooping enable
[SwitchA-vlan10] quit
```

Create VLAN 2 and enable MLD snooping in the VLAN.

```
[SwitchA] vlan 2
[SwitchA-vlan2] mld-snooping enable
[SwitchA-vlan2] quit
```

The configuration for VLAN 3 and VLAN 4 is similar. (Details not shown.)

Configure GigabitEthernet 1/0/2 as a hybrid port. Configure VLAN 2 as the default VLAN. Configure GigabitEthernet 1/0/2 to permit packets of VLAN 2 to pass and untag the packets when forwarding them.

```
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type hybrid
[SwitchA-GigabitEthernet1/0/2] port hybrid pvid vlan 2
[SwitchA-GigabitEthernet1/0/2] port hybrid vlan 2 untagged
[SwitchA-GigabitEthernet1/0/2] port hybrid vlan 10 untagged
[SwitchA-GigabitEthernet1/0/2] quit
```

The configuration for GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 is similar. (Details not shown.)

Configure VLAN 10 as an IPv6 multicast VLAN.

```
[SwitchA] multicast-vlan ipv6 10
```

Assign GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to IPv6 multicast VLAN 10.

```
[SwitchA-ipv6-mvlan-10] port gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[SwitchA-ipv6-mvlan-10] quit
```

Assign GigabitEthernet 1/0/4 to IPv6 multicast VLAN 10.

```
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port multicast-vlan ipv6 10
[SwitchA-GigabitEthernet1/0/4] quit
```

Verifying the configuration

Display the IPv6 multicast VLAN information on Switch A.

```
[SwitchA] display multicast-vlan ipv6
Total 1 IPv6 multicast-vlan(s)
IPv6 Multicast vlan 10
  subvlan list:
    no subvlan
  port list:
```

```

GE1/0/2                GE1/0/3                GE1/0/4
# Display the MLD snooping multicast group information on Switch A.
[SwitchA] display mld-snooping group
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):10.
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port(s).
    GE1/0/1                (D)
IP group(s):the following ip group(s) match to one mac group.
IP group address:FF1E::101
  (::, FF1E::101):
    Host port(s):total 3 port(s).
      GE1/0/2                (D)
      GE1/0/3                (D)
      GE1/0/4                (D)
MAC group(s):
  MAC group address:3333-0000-0101
    Host port(s):total 3 port(s).
      GE1/0/2
      GE1/0/3
      GE1/0/4

```

The output shows that MLD snooping is maintaining router ports and member ports in VLAN 10.

Configuring IPv6 multicast routing and forwarding (available only on the HP 5500 EI)

Overview

In IPv6 multicast implementations, the following types of tables implement multicast routing and forwarding:

- **Multicast routing table of an IPv6 multicast routing protocol**—Each IPv6 multicast routing protocol has its own multicast routing table, such as IPv6 PIM routing table.
- **General IPv6 multicast routing table**—The multicast routing information of different IPv6 multicast routing protocols forms a general IPv6 multicast routing table.
- **IPv6 multicast forwarding table**—The IPv6 multicast forwarding table guides the forwarding of IPv6 multicast packets.

An IPv6 multicast forwarding table consists of a set of (S, G) entries. Each entry indicates the routing information for delivering multicast data from a multicast source to a multicast group. If a router supports multiple IPv6 multicast protocols, its IPv6 multicast routing table will include routes that these protocols have generated. The router chooses the optimal route from the IPv6 multicast routing table based on the configured multicast routing and forwarding policy and installs the route entry into its IPv6 multicast forwarding table.

The term "router" in this document refers to both routers and Layer 3 switches.

The term "interface" in the IPv6 multicast routing and forwarding features collectively refers to Layer 3 interfaces, including VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

RPF check mechanism

An IPv6 multicast routing protocol relies on the existing IPv6 unicast routing information or IPv6 MBGP routes in creating IPv6 multicast routing entries. When creating IPv6 multicast routing table entries, an IPv6 multicast routing protocol uses the reverse path forwarding (RPF) check mechanism to ensure IPv6 multicast data delivery along the correct path. The RPF check mechanism also helps avoid data loops caused by various reasons.

An RPF check is based on one of the following routing tables:

- **IPv6 unicast routing table**—Contains the shortest path to each destination subnet

- **IPv6 MBGP routing table**—Contains IPv6 multicast routing information

When a router performs an RPF check, it searches its IPv6 unicast routing table and IPv6 MBGP routing table at the same time. The specific process is as follows:

1. The router chooses each optimal route from the IPv6 unicast routing table and the IPv6 MBGP routing table:
 - The router searches its IPv6 unicast routing table by using the IPv6 address of the packet source as the destination address and automatically selects the optimal route as the RPF route. The outgoing interface in the corresponding routing entry is the RPF interface and the next hop is the RPF neighbor. The router considers the path along which the IPv6 multicast packet from the RPF neighbor arrived on the RPF interface to be the shortest path that leads back to the source.
 - The router automatically chooses an optimal IPv6 MBGP route by searching its MBGP routing table, and using the IPv6 address of the packet source as the destination address. The outgoing interface in the corresponding routing entry is the RPF interface and the next hop is the RPF neighbor.
2. The router selects one of these optimal routes as the RPF route. The selection process is as follows:
 - If configured to use the longest match principle, the router selects the longest match route from these optimal routes. If these routes have the same prefix length, the router selects the route with a higher priority. If these routes have the same priority, the router selects the IPv6 MBGP route as the RPF route.
 - If not configured to use the longest match principle, the router selects the route with a higher priority. If these routes have the same priority, the router selects the IPv6 MBGP route as the RPF route.

The term "packet source" can mean different things in different situations:

- For a packet that traveling along the shortest path tree (SPT) from the multicast source to the receivers or the rendezvous point (RP), the packet source for RPF check is the multicast source.
- For a packet that traveling along the rendezvous point tree (RPT) from the RP to the receivers, or along the source-side RPT from the multicast source to the RP, the packet source for RPF check is the RP.
- For a bootstrap message from the bootstrap router (BSR), the packet source for RPF check is the BSR.

For more information about the concepts of SPT, RPT, source-side RPT, RP, and BSR, see "[Configuring IPv6 PIM \(available only on the HP 5500 EI\)](#)."

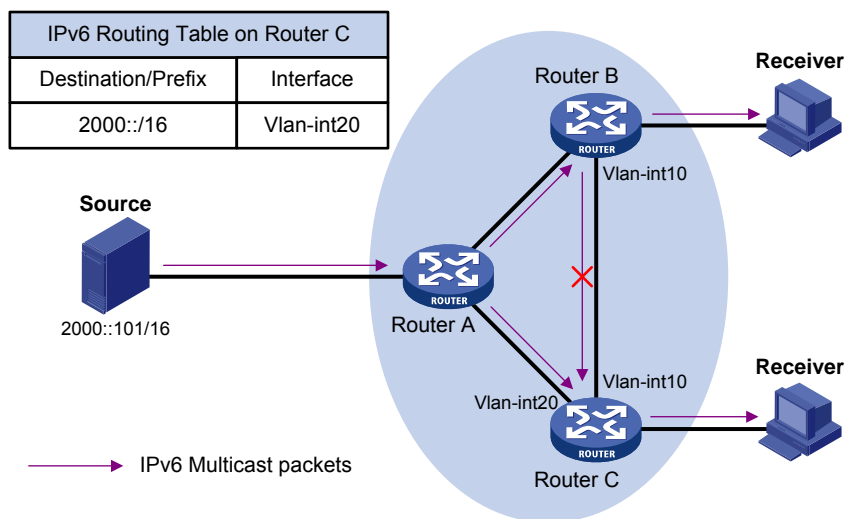
RPF check implementation in IPv6 multicast

Implementing an RPF check on each received IPv6 multicast data packet would heavily burden the router. The use of an IPv6 multicast forwarding table is the solution to this issue. When creating an IPv6 multicast routing entry and an IPv6 multicast forwarding entry for an IPv6 multicast packet, the router sets the RPF interface of the packet as the incoming interface of the (S, G) entry. After receiving an (S, G) IPv6 multicast packet, the router first searches its IPv6 multicast forwarding table:

1. If the corresponding (S, G) entry does not exist in the IPv6 multicast forwarding table, the packet undergoes an RPF check. The router creates an IPv6 multicast routing entry based on the relevant routing information and installs the entry into the IPv6 multicast forwarding table, with the RPF interface as the incoming interface.
 - If the interface that received the packet is the RPF interface, the RPF check succeeds and the router forwards the packet to all the outgoing interfaces.
 - If the interface that received the packet is not the RPF interface, the RPF check fails and the router discards the packet.
2. If the corresponding (S, G) entry exists, and the interface that received the packet is the incoming interface, the router forwards the packet to all the outgoing interfaces.
3. If the corresponding (S, G) entry exists, but the interface that received the packet is not the incoming interface in the IPv6 multicast forwarding table, the IPv6 multicast packet undergoes an RPF check.
 - If the RPF interface is the incoming interface of the (S, G) entry, this means the (S, G) entry is correct but the packet arrived from a wrong path. The packet will be discarded.
 - If the RPF interface is not the incoming interface, this means that the (S, G) entry has expired, and the router replaces the incoming interface with the RPF interface. If the interface on which the packet arrived is the RPF interface, the router forwards the packet to all the outgoing interfaces. Otherwise it discards the packet.

Assume that IPv6 unicast routes are available in the network, IPv6 MBGP is not configured, and IPv6 multicast packets travel along the SPT from the multicast source to the receivers, as shown in Figure 82. The IPv6 multicast forwarding table on Router C contains the (S, G) entry, with VLAN-interface 20 as the RPF interface.

Figure 82 RPF check process



- When an IPv6 multicast packet arrives on VLAN-interface 20 of Router C, because the interface is the incoming interface of the (S, G) entry, the router forwards the packet to all outgoing interfaces.

- When an IPv6 multicast packet arrives on VLAN-interface 10 of Router C, because the interface is not the incoming interface of the (S, G) entry, the router performs an RPF check on the packet. The router searches its IPv6 unicast routing table and finds that the outgoing interface to Source (the RPF interface) is VLAN-interface 20. This means that the (S, G) entry is correct and the packet arrived along a wrong path. The RPF check fails and the packet is discarded.

Configuration task list

Task	Remarks	
Enabling IPv6 multicast routing	Required	
Configuring IPv6 multicast routing and forwarding	Configuring an IPv6 multicast routing policy	Optional
	Configuring an IPv6 multicast forwarding range	Optional
	Configuring the IPv6 multicast forwarding table size	Optional

Enabling IPv6 multicast routing

Before you configure any Layer 3 IPv6 multicast functionality, you must enable IPv6 multicast routing.

To enable IPv6 multicast routing:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IPv6 multicast routing.	multicast ipv6 routing-enable	Disabled by default.

Configuring IPv6 multicast routing and forwarding

Before you configure IPv6 multicast routing and forwarding, complete the following tasks:

- Enable IPv6 forwarding and configure an IPv6 unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Configure IPv6 PIM-DM or IPv6 PIM-SM.
- Determine the maximum number of downstream nodes for a single entry in the IPv6 multicast forwarding table.
- Determine the maximum number of entries in the IPv6 multicast forwarding table.

Configuring an IPv6 multicast routing policy

You can configure the router to determine the RPF route based on the longest match principle. For more information about RPF route selection, see "[RPF check mechanism](#)."

By configuring per-source or per-source-and-group load splitting, you can optimize the traffic delivery when multiple IPv6 multicast data streams are handled.

To configure an IPv6 multicast routing policy:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the device to select the RPF route based on the longest match.	multicast ipv6 longest-match	Optional. The route with the highest priority is selected as the RPF route by default.
3. Configure IPv6 multicast load splitting.	multicast ipv6 load-splitting { source source-group }	Optional. Disabled by default. This command does not take effect in IPv6 BIDIR-PIM.

Configuring an IPv6 multicast forwarding range

IPv6 multicast packets do not travel infinitely in a network. The IPv6 multicast data of each IPv6 multicast group must be transmitted within a definite scope.

You can configure the forwarding boundary for a specific IPv6 multicast group or an IPv6 multicast group with the scope field in its group address being specified on all interfaces that support IPv6 multicast forwarding. A multicast forwarding boundary sets the boundary condition for the IPv6 multicast groups in the specified range or scope. If the destination address of an IPv6 multicast packet matches the set boundary condition, the packet will not be forwarded. Once an IPv6 multicast boundary is configured on an interface, this interface can no longer forward IPv6 multicast packets (including those sent from the local device) or receive IPv6 multicast packets.

To configure an IPv6 multicast forwarding range:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure an IPv6 multicast forwarding boundary.	multicast ipv6 boundary { <i>ipv6-group-address</i> <i>prefix-length</i> scope { <i>scope-id</i> admin-local global organization-local site-local } }	No forwarding boundary by default.

Configuring the IPv6 multicast forwarding table size

The switch maintains the corresponding forwarding entry for each IPv6 multicast packet that it receives. Excessive IPv6 multicast routing entries, however, can exhaust the switch's memory and cause lower

performance. You can set a limit on the number of entries in the IPv6 multicast forwarding table based on the actual networking situation and the performance requirements. If the configured maximum number of IPv6 multicast forwarding table entries is smaller than the current value, the entries in excess are not immediately deleted. Instead, the IPv6 multicast routing protocol that runs on the switch deletes them. The switch no longer adds new IPv6 multicast forwarding entries until the number of existing IPv6 multicast forwarding entries comes down below the configured value.

When the switch forwards IPv6 multicast traffic, it replicates a copy of the IPv6 multicast traffic for each downstream node and forwards the traffic. Each of these downstream nodes forms a branch of the IPv6 multicast distribution tree. You can configure the maximum number of downstream nodes (the maximum number of outgoing interfaces) for a single entry in the IPv6 multicast forwarding table to lessen the burden on the switch for replicating IPv6 multicast traffic. If the configured maximum number of downstream nodes for a single IPv6 multicast forwarding entry is smaller than the current number, the downstream nodes in excess are not deleted immediately. Instead, the IPv6 multicast routing protocol deletes them. The switch no longer adds new IPv6 multicast forwarding entries for newly added downstream nodes until the number of existing downstream nodes comes down below the configured value.

To configure the IPv6 multicast forwarding table size:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the maximum number of entries in the IPv6 multicast forwarding table.	multicast ipv6 forwarding-table route-limit <i>limit</i>	Optional. 1000 by default.
3. Configure the maximum number of downstream nodes for a single IPv6 multicast forwarding entry.	multicast ipv6 forwarding-table downstream-limit <i>limit</i>	Optional. 128 by default.

Displaying and maintaining IPv6 multicast routing and forwarding

⚠ CAUTION:

The **reset** commands might cause IPv6 multicast data transmission failures.

To display and maintain IPv6 multicast routing and forwarding:

Task	Command	Remarks
Display the IPv6 multicast boundary information.	display multicast ipv6 boundary { group [<i>ipv6-group-address</i> [<i>prefix-length</i>]] scope [<i>scope-id</i>] } [interface <i>interface-type interface-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

Task	Command	Remarks
Display the information of the IPv6 multicast forwarding table.	display multicast ipv6 forwarding-table [<i>ipv6-source-address</i> [<i>prefix-length</i>] <i>ipv6-group-address</i> [<i>prefix-length</i>] incoming-interface { <i>interface-type</i> <i>interface-number</i> register } outgoing-interface { exclude include match } { <i>interface-type</i> <i>interface-number</i> register } statistics slot <i>slot-number</i>] * [port-info] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the DF information of the IPv6 multicast forwarding table.	display multicast ipv6 forwarding-table df-info [<i>rp-address</i>] [slot <i>slot-number</i>] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the information of the IPv6 multicast routing table.	display multicast ipv6 routing-table [<i>ipv6-source-address</i> [<i>prefix-length</i>] <i>ipv6-group-address</i> [<i>prefix-length</i>] incoming-interface { <i>interface-type</i> <i>interface-number</i> register } outgoing-interface { exclude include match } { <i>interface-type</i> <i>interface-number</i> register }] * [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the RPF route information of the specified IPv6 multicast source.	display multicast ipv6 rpf-info <i>ipv6-source-address</i> [<i>ipv6-group-address</i>] [[{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Clear forwarding entries from the IPv6 multicast forwarding table.	reset multicast ipv6 forwarding-table { { <i>ipv6-source-address</i> [<i>prefix-length</i>] <i>ipv6-group-address</i> [<i>prefix-length</i>] incoming-interface { <i>interface-type</i> <i>interface-number</i> register } } } * all }	Available in user view. When a forwarding entry is deleted from the IPv6 multicast forwarding table, the corresponding routing entry is also deleted from the IPv6 multicast routing table.
Clear routing entries from the IPv6 multicast routing table.	reset multicast ipv6 routing-table { { <i>ipv6-source-address</i> [<i>prefix-length</i>] <i>ipv6-group-address</i> [<i>prefix-length</i>] incoming-interface { <i>interface-type</i> <i>interface-number</i> register } } } * all }	Available in user view. When a routing entry is deleted from the IPv6 multicast routing table, the corresponding forwarding entry is also deleted from the IPv6 multicast forwarding table.

For more information about designated forwarder (DF), see "[Configuring IPv6 PIM \(available only on the HP 5500 EI\)](#)."

Troubleshooting IPv6 multicast policy configuration

Abnormal termination of IPv6 multicast data

Symptom

- A host sends an MLD report announcing its joining an IPv6 multicast group (G). However, no member information about the IPv6 multicast group (G) exists on the intermediate router. The intermediate router can receive IPv6 multicast packets successfully, but the packets cannot reach the stub network.
- The interface of the intermediate router receives the IPv6 multicast packets, but no corresponding (S, G) entry exists in the IPv6 PIM routing table.

Analysis

- The **multicast ipv6 boundary** command filters IPv6 multicast packets received on an interface. If an IPv6 multicast packet fails to match the IPv6 ACL rule of this command, IPv6 PIM will create no routing entry.
- In addition, the **source-policy** command in IPv6 PIM filters received IPv6 multicast packets. If an IPv6 multicast packet fails to match the IPv6 ACL rule of this command, IPv6 PIM will not create a routing entry, either.

Solution

1. Use the **display current-configuration** command to display the IPv6 ACL rule configured on the multicast forwarding boundary. Change the IPv6 ACL rule used in the **multicast ipv6 boundary** command so that the source IP address of the IPv6 multicast packets and the IPv6 multicast group address can both match the IPv6 ACL rule.
2. View the configuration of the multicast filter. Use the **display current-configuration** command to display the configuration of the IPv6 multicast filter. Change the IPv6 ACL rule used in the **source-policy** command so that the source IP address of the IPv6 multicast packets and the IPv6 multicast group address can both match the IPv6 ACL rule.

Configuring MLD (available only on the HP 5500 EI)

Overview

An IPv6 router uses the Multicast Listener Discovery (MLD) protocol to discover the presence of multicast listeners on the directly attached subnets. Multicast listeners are nodes that want to receive IPv6 multicast packets.

Through MLD, the router can determine whether any IPv6 multicast listeners exist on the directly connected subnets, put corresponding records in the database, and maintain timers related to IPv6 multicast addresses.

Routers running MLD use an IPv6 unicast link-local address as the source address to send MLD messages. MLD messages are Internet Control Message Protocol for IPv6 (ICMPv6) messages. All MLD messages are confined to the local subnet, with a hop count of 1.

The term "router" in this document refers to both routers and Layer 3 switches.

The term "interface" in this chapter collectively refers to Layer 3 interfaces, including VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

MLD versions

- MLDv1 (defined in RFC 2710), which is derived from IGMPv2.
- MLDv2 (defined in RFC 3810), which is derived from IGMPv3.

All MLD versions support the Any-Source Multicast (ASM) model. In addition, MLDv2 can directly implement the Source-Specific Multicast (SSM) model, but MLDv1 must work with the MLD SSM mapping function to implement SSM service.

For more information about the ASM and SSM models, see "[Multicast overview](#)."

How MLDv1 works

MLDv1 implements IPv6 multicast listener management based on the query/response mechanism.

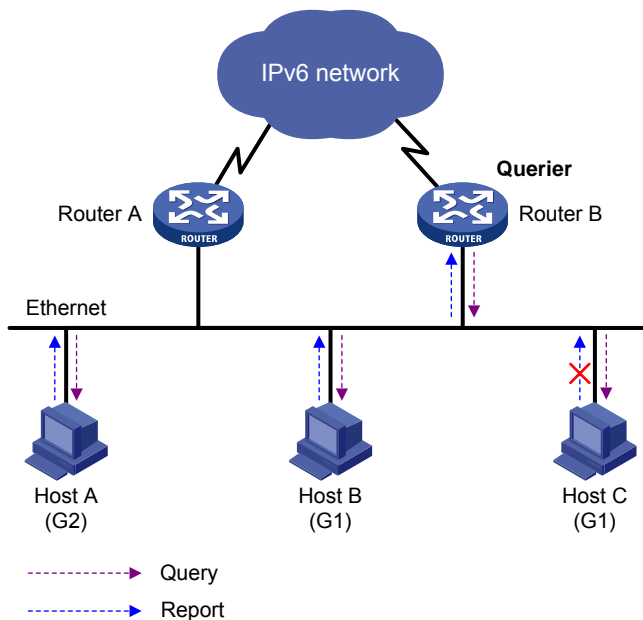
MLD querier election

All IPv6 multicast routers on the same subnet can monitor MLD listener report messages (often called "reports") from hosts, but only one router is needed to send MLD query messages (often called "queries"). The querier election mechanism determines which router will act as the MLD querier on the subnet.

1. Initially, every MLD router assumes itself as the querier and sends MLD general query messages (often called "general queries") to all hosts and routers on the local subnet. The destination address is FF02::1.
2. After receiving a general query, every MLD router compares the source IPv6 address of the query message with its own interface address. After comparison, the router with the lowest IPv6 address wins the querier election and all other routers become non-queriers.
3. All the non-queriers start a timer called the "other querier present timer." If a router receives an MLD query from the querier before the timer expires, it resets this timer. Otherwise, it assumes that the querier has timed out and initiates a new querier election process.

Joining an IPv6 multicast group

Figure 83 MLD queries and reports



Assume that Host B and Host C will receive IPv6 multicast data addressed to IPv6 multicast group G1, and Host A will receive IPv6 multicast data addressed to G2, as shown in Figure 83. The following process describes how the hosts join the IPv6 multicast groups and how the MLD querier (Router B in the figure) maintains the IPv6 multicast group memberships:

1. The hosts send unsolicited MLD reports to the addresses of the IPv6 multicast groups that they will join, without having to wait for the MLD queries from the MLD querier.
2. The MLD querier periodically multicasts MLD queries (with the destination address of FF02::1) to all hosts and routers on the local subnet.

3. After receiving a query message, Host B or Host C (the delay timer of whichever expires first) sends an MLD report to the IPv6 multicast group address of G1, to announce its membership for G1. Assume that Host B sends the report message. After hearing the report from Host B, Host C, which is on the same subnet as Host B, suppresses its own report for G1, because the MLD routers (Router A and Router B) have already known that at least one host on the local subnet is interested in G1. This mechanism, known as the "MLD report suppression", helps reduce traffic on the local subnet.
4. At the same time, because Host A is interested in G2, it sends a report to the IPv6 multicast group address of G2.
5. Through the query/report process, the MLD routers learn that members of G1 and G2 are attached to the local subnet, and the IPv6 multicast routing protocol (for example, IPv6 PIM) that is running on the routers generates (*, G1) and (*, G2) multicast forwarding entries. These entries will be the basis for subsequent IPv6 multicast forwarding, where * represents any IPv6 multicast source.
6. When the IPv6 multicast data addressed to G1 or G2 reaches an MLD router, because the (*, G1) and (*, G2) multicast forwarding entries exist on the MLD router, the router forwards the IPv6 multicast data to the local subnet, and then the receivers on the subnet receive the data.

Leaving an IPv6 multicast group

When a host leaves a multicast group, the following occur:

1. The host sends an MLD done message to all IPv6 multicast routers on the local subnet. The destination address is FF02::2.
2. After receiving the MLD done message, the querier sends a configurable number of multicast-address-specific queries to the group that the host is leaving. The destination address field and group address field of the message are both filled with the address of the IPv6 multicast group that is being queried.
3. One of the remaining members (if any on the subnet) of the group being queried should send a report within the time of the maximum response delay set in the query messages.
4. If the querier receives a report for the group within the maximum response delay time, it will maintain the memberships of the IPv6 multicast group. Otherwise, the querier will assume that no hosts on the subnet are still interested in IPv6 multicast traffic addressed to that group and will stop maintaining the memberships of the group.

How MLDv2 works

Compared with MLDv1, MLDv2 provides the following new features:

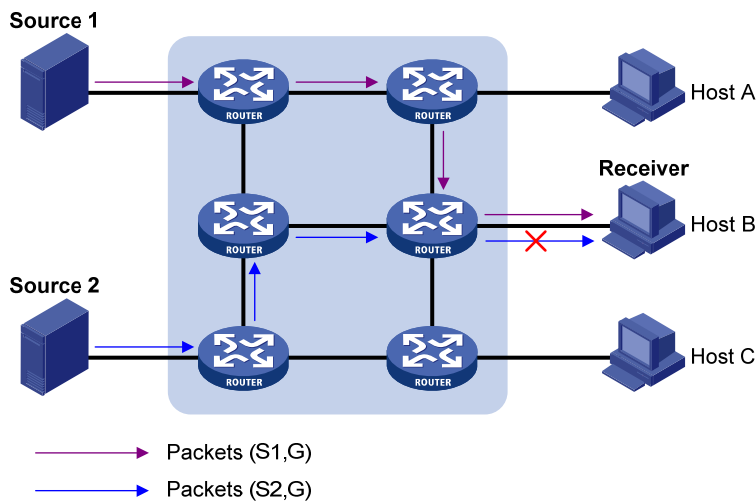
IPv6 multicast group filtering

MLDv2 has introduced IPv6 multicast source filtering modes (Include and Exclude), so that a host not only can join a designated IPv6 multicast group, but also can specify to receive or reject multicast data from designated IPv6 multicast sources. When a host joins an IPv6 multicast group, one of the following situations occurs:

- If it expects IPv6 multicast data from specific IPv6 multicast sources like S1, S2, ..., it sends a report with Filter-Mode denoted as "Include Sources (S1, S2, ...)."
- If it does not expect IPv6 multicast data from specific IPv6 multicast sources like S1, S2, ..., it sends a report with Filter-Mode denoted as "Exclude Sources (S1, S2, ...)."

As shown in Figure 84, the network comprises two IPv6 multicast sources, Source 1 (S1) and Source 2 (S2), both of which can send IPv6 multicast data to IPv6 multicast group G. Host B is interested only in the IPv6 multicast data that Source 1 sends to G but not in the data from Source 2.

Figure 84 Flow paths of multicast-address-and-source-specific multicast traffic



In the case of MLDv1, Host B cannot select IPv6 multicast sources when it joins IPv6 multicast group G. Therefore, IPv6 multicast streams from both Source 1 and Source 2 will flow to Host B whether it needs them or not.

When MLDv2 is running on the hosts and routers, Host B can explicitly express its interest in the IPv6 multicast data that Source 1 sends to G (denoted as (S1, G)), rather than the IPv6 multicast data that Source 2 sends to G (denoted as (S2, G)). Thus, only IPv6 multicast data from Source 1 will be delivered to Host B.

MLD state

A multicast router that is running MLDv2 maintains the multicast address state per multicast address per attached subnet. The multicast address state consists of the following information:

- **Filter mode**—The router keeps tracing the Include or Exclude state.
- **List of sources**—The router keeps tracing the newly added or deleted IPv6 multicast source.
- **Timers**—Filter timers, including the time that the router waits before switching to the Include mode after an IPv6 multicast address times out, the source timer for source recording, and so on.

Receiver host state listening

By listening to the state of receiver hosts, a multicast router running MLDv2 records and maintains information of hosts joining the source group on the attached subnet.

MLD messages

The following descriptions are based on MLDv2 messages.

MLD query message

An MLD querier learns the multicast listening state of neighbor interfaces by sending MLD query messages. The dark area in [Figure 85](#) shows the MLDv1 message format.

Figure 85 MLDv2 query message format

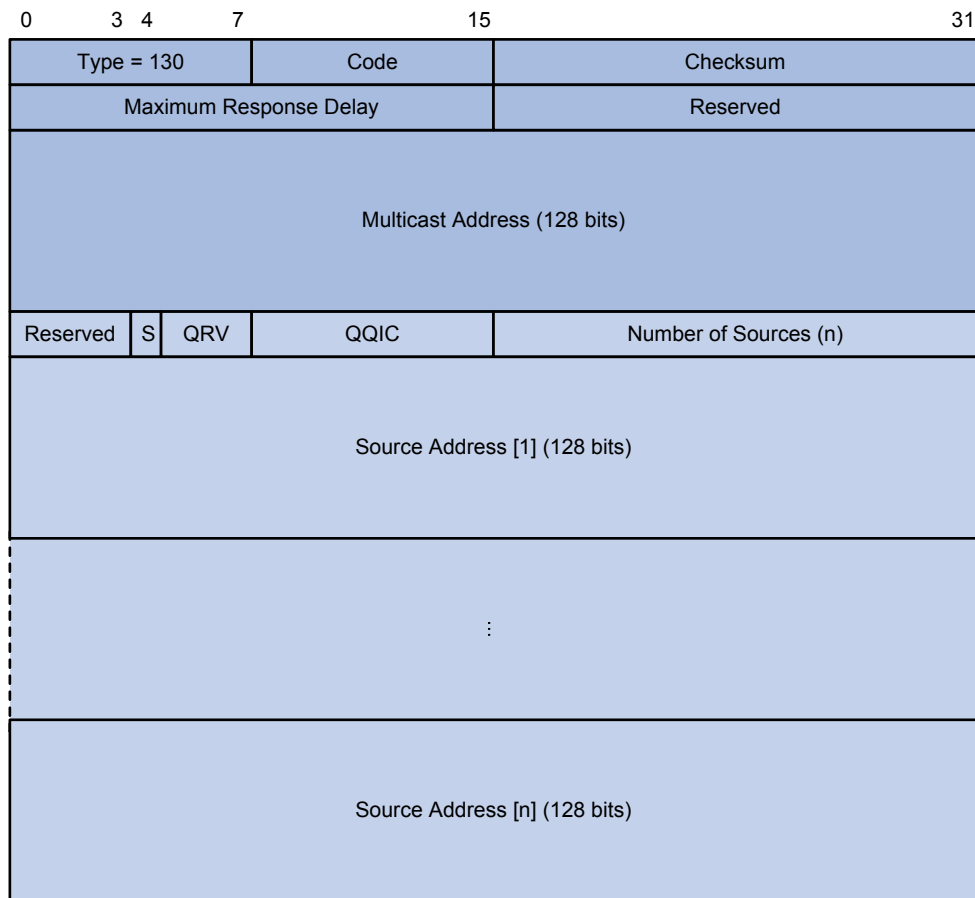


Table 9 MLDv2 query message field description

Field	Description
Type = 130	Message type. For a query message, this field is set to 130.
Code	Initialized to zero.
Checksum	Standard IPv6 checksum.
Maximum Response Delay	Maximum response delay allowed before a host sends a report message.
Reserved	Reserved field and initialized to zero.

Field	Description
Multicast Address	<ul style="list-style-type: none"> This field is set to 0 in a general query message. It is set to a specific IPv6 multicast address in a multicast-address-specific query message or multicast-address-and-source-specific query message.
S	Flag indicating whether a router updates the timer for suppression after receiving a query message.
QRV	Querier's Robustness Variable.
QQIC	Querier's Query Interval Code.
Number of Sources	<ul style="list-style-type: none"> This field is set to 0 in a general query message or a multicast-address-specific query message. This field represents the number of source addresses in a multicast-address-and-source-specific query message.
Source Address(i)	IPv6 multicast source address in a multicast-address-specific query message. (i = 1, 2, .., n, where n represents the number of multicast source addresses.)

MLD report message

A host sends an MLD report message to report the current multicast listening state. [Figure 86](#) shows the MLD report message format.

Figure 86 MLDv2 report message format

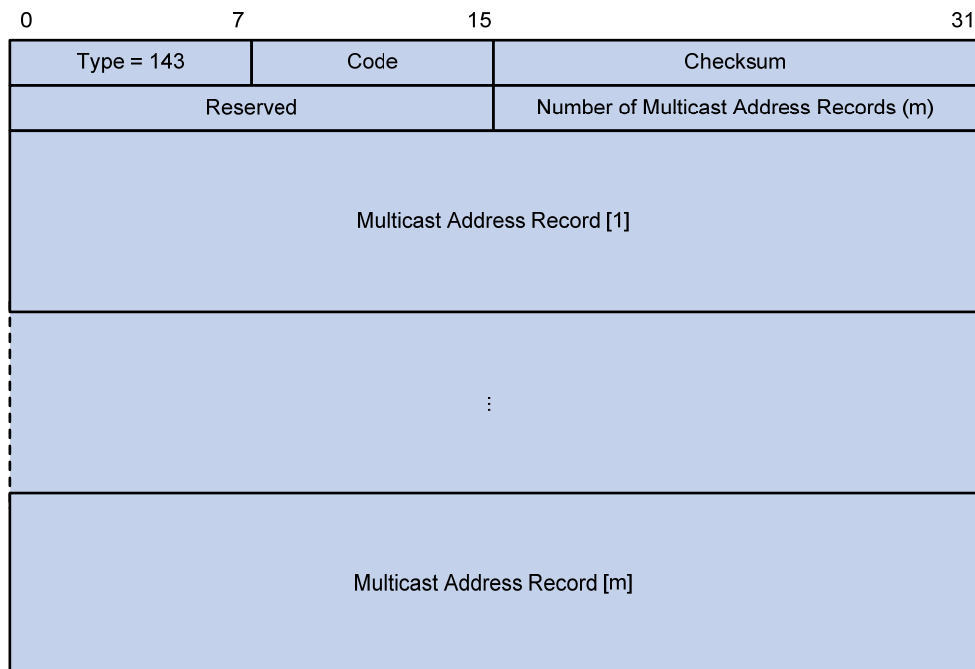


Table 10 MLDv2 report message field description

Field	Description
Type = 143	Message type. For a report message, this field is set to 143.

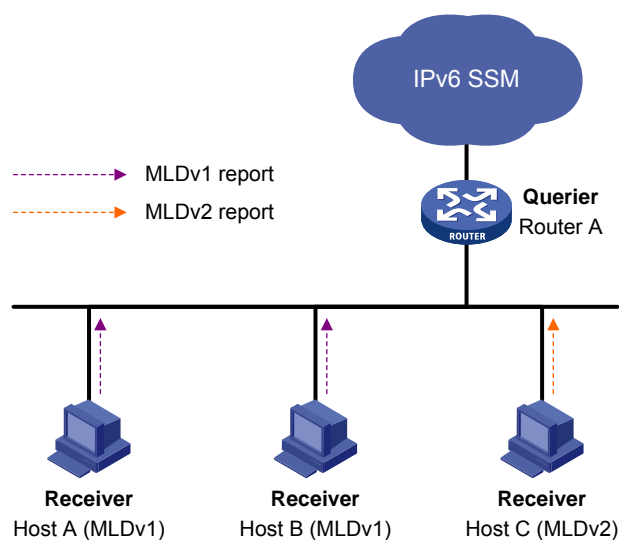
Field	Description
Reserved	The Reserved fields are set to 0 on transmission and ignored on reception.
Checksum	Standard IPv6 checksum.
Number of Multicast Address Records	This field indicates how many IPv6 multicast address records are present in this report message.
Multicast Address Record(i)	This field represents information of each IPv6 multicast address the host listens to on the interface from which the report message is sent, including record type, IPv6 multicast address, and IPv6 multicast source address on the sender. (i= 1, 2, ... m, where m represents the number of IPv6 multicast address records).

MLD SSM mapping

The MLD SSM mapping feature enables you to configure static MLD SSM mappings on the last hop router to provide SSM support for receiver hosts that are running MLDv1. The SSM model assumes that the last hop router has identified the desired IPv6 multicast sources when receivers join IPv6 multicast groups.

- When an MLDv2 enabled host joins a multicast group, it can explicitly specify one or more multicast sources in its MLDv2 report.
- An MLDv1-enabled host, however, cannot specify multicast source addresses in its MLDv1 report. You must configure the MLD SSM mapping feature to translate the (*, G) information in the MLDv1 report into (G, INCLUDE, (S1, S2...)) information.

Figure 87 Network diagram



On the IPv6 SSM network in [Figure 87](#), Host A and Host B are running MLDv1 and Host C is running MLDv2. To provide SSM service for Host A and Host B, you must configure the MLD SSM mapping feature on Router A.

With the MLD SSM mapping feature configured, when Router A receives an MLDv1 report, it checks the IPv6 multicast group address G carried in the message.

- If G is not in the IPv6 SSM group range, Router A cannot provide the SSM service but can provide the ASM service.
- If G is in the IPv6 SSM group range but no MLD SSM mappings have been configured for the IPv6 multicast group G on Router A, Router A cannot provide SSM service and drops the packet.
- If G is in the IPv6 SSM group range, and the MLD SSM mappings have been configured on Router A for multicast group G, Router A translates the (*, G) information in the MLD report into (G, INCLUDE, (S1, S2...)) information based on the configured MLD SSM mappings and provides SSM service accordingly.

NOTE:

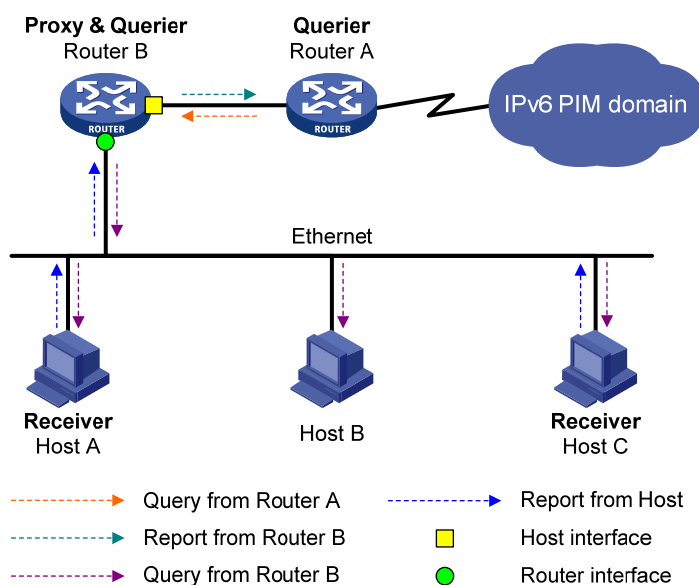
The MLD SSM mapping feature does not process MLDv2 reports.

For more information about the IPv6 SSM group range, see "[Configuring IPv6 PIM \(available only on the HP 5500 EI\)](#)."

MLD proxying

In some simple tree-shaped topologies, you do not need to configure complex IPv6 multicast routing protocols, such as IPv6 PIM, on the boundary devices. Instead, you can configure MLD proxying on these devices. With MLD proxying configured, the device serves as a proxy for the downstream hosts to send MLD messages, maintain group memberships, and implement IPv6 multicast forwarding based on the memberships. In this case, the MLD proxy device is a host but no longer an IPv6 PIM neighbor to the upstream device.

Figure 88 Network diagram



As shown in [Figure 88](#), an MLD proxy device has the following types of interfaces:

- **Upstream interface**—Also called the "proxy interface." A proxy interface is an interface on which MLD proxying is configured. It is in the direction toward the root of the multicast forwarding tree. An upstream interface acts as a host that is running MLD, and is also called a "host interface."
- **Downstream interface**—An interface that is running MLD and not in the direction toward the root of the multicast forwarding tree. A downstream interface acts as a router that is running MLD, and is also called a "router interface."

A device with MLD proxying configured maintains a group membership database, which stores the group memberships on all the downstream interfaces in this database. Each entry comprises the multicast address, filter mode, and source list. Such an entry is a collection of members in the same multicast group on each downstream interface.

A proxy device performs host functions on the upstream interface based on the database. It responds to the queries according to the information in the database or sends join/leave messages when the database changes. The proxy device performs router functions on the downstream interfaces by participating in the querier election, sending queries, and maintaining memberships based on the reports.

Protocols and standards

- RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*
- RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*
- RFC 4605, *Internet Group Management Protocol (IGMP)/Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")*

MLD configuration task list

Task	Remarks	
Configuring basic MLD functions	Enabling MLD	Required
	Configuring the MLD version	Option
	Configuring static joining	Optional
	Configuring an IPv6 multicast group filter	Optional
	Setting the maximum number of IPv6 multicast groups that an interface can join	Optional
Adjusting MLD performance	Configuring Router-Alert option handling methods	Optional
	Configuring MLD query and response parameters	Optional
	Configuring MLD fast-leave processing	Optional
	Enabling the MLD host tracking function	Optional
	Setting the DSCP value for MLD messages	Optional

Task	Remarks	
Configuring MLD SSM mapping	Enabling MLD SSM mapping	Optional
	Configuring MLD SSM mappings	Optional
Configuring MLD proxying	Enabling MLD proxying	Optional
	Configuring IPv6 multicast forwarding on a downstream interface	Optional

NOTE:

- In MLD view, the configuration is effective globally. In interface view, the configuration is effective on only the current interface.
- If no configuration is performed in interface view, the global configuration in MLD view will apply to that interface. Configurations performed in interface view take precedence over those performed in MLD view.

Configuring basic MLD functions

Before you configure basic MLD functions, complete the following tasks:

- Enable IPv6 forwarding and configure an IPv6 unicast routing protocol so that all devices in the domain can be interoperable at the network layer.
- Configure IPv6 PIM-DM or IPv6 PIM-SM.
- Determine the MLD version.
- Determine the IPv6 multicast group address and IPv6 multicast source address for static group member configuration.
- Determine the ACL rule for IPv6 multicast group filtering.
- Determine the maximum number of IPv6 multicast groups that an interface can join.

Enabling MLD

Enable MLD on the interface on which IPv6 multicast group memberships will be created and maintained.

To enable MLD:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IPv6 multicast routing.	multicast ipv6 routing-enable	Disable by default
3. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable MLD.	mld enable	Disabled by default

For more information about the **multicast ipv6 routing-enable** command, see *IP Multicast Command Reference*.

Configuring the MLD version

Because MLD message types and formats vary with MLD versions, the same MLD version should be configured for all routers on the same subnet before MLD can work properly.

Configuring an MLD version globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD view.	mld	N/A
3. Configure an MLD version globally.	version <i>version-number</i>	MLDv1 by default

Configuring an MLD version on an interface

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure an MLD version on the interface.	mld version <i>version-number</i>	MLDv1 by default

Configuring static joining

After an interface is configured as a static member of an IPv6 multicast group or an IPv6 multicast source and group, it will act as a virtual member of the IPv6 multicast group to receive IPv6 multicast data addressed to that IPv6 multicast group for the purpose of testing IPv6 multicast data forwarding.

Configuration guidelines

- Before you can configure an interface of an IPv6 PIM-SM device as a static member of an IPv6 multicast group or an IPv6 multicast source and group, if the interface is IPv6 PIM-SM enabled, it must be an IPv6 PIM-SM DR. If this interface is MLD enabled but not IPv6 PIM-SM enabled, it must be an MLD querier. For more information about IPv6 PIM-SM and a DR, see "[Configuring IPv6 PIM \(available only on the HP 5500 EI\)](#)."
- A static member port does not respond to queries from the MLD querier. When you configure an interface as a static member port or remove this configuration on the interface, the interface does not unsolicitedly send any MLD report or an MLD done message. In other words, the interface is not a real member of the IPv6 multicast group or the IPv6 multicast and source group.

Configuration procedure

To configure a static member of an IPv6 multicast group or an IPv6 multicast source and group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure a static member of an IPv6 multicast group or an IPv6 multicast source and group.	mld static-group <i>ipv6-group-address</i> [source <i>ipv6-source-address</i>]	By default, an interface is not a static member of any IPv6 multicast group or IPv6 multicast source and group.

Configuring an IPv6 multicast group filter

To restrict the hosts on the network attached to an interface from joining certain IPv6 multicast groups, you can set an IPv6 ACL rule on the interface so that the interface maintains only the IPv6 multicast groups matching the criteria.

To configure an IPv6 multicast group filter:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure an IPv6 multicast group filter.	mld group-policy <i>acl6-number</i> [<i>version-number</i>]	By default, no IPv6 group filter is configured on the interface. That is, hosts on the current interface can join any valid multicast group.

Setting the maximum number of IPv6 multicast groups that an interface can join

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the maximum number of IPv6 multicast groups that the interface can join.	mld group-limit <i>limit</i>	1000 by default.

NOTE:

This configuration takes effect for dynamically joined IPv6 multicast groups but not the statically configured multicast groups.

Adjusting MLD performance

For the configuration tasks in this section:

- In MLD view, the configuration is effective globally. In interface view, the configuration is effective only on the current interface.
- If the same function or parameter is configured in both MLD view and interface view, the configuration performed in interface view is given priority, regardless of the configuration order.

Configuration prerequisites

Before adjusting MLD performance, complete the following tasks:

- Enable IPv6 forwarding and configure an IPv6 unicast routing protocol so that all devices in the domain can be interoperable at the network layer.
- Configure basic MLD functions.
- Determine the startup query interval.
- Determine the startup query count.
- Determine the MLD query interval.
- Determine the MLD querier's robustness variable.
- Determine the maximum response delay of MLD general query messages.
- Determine the MLD last listener query interval.
- Determine the MLD other querier present interval.
- Determine the DSCP value for MLD messages.

Configuring Router-Alert option handling methods

MLD queries include multicast-address-specific queries and multicast-address-and-source-specific queries, and IPv6 multicast groups change dynamically, so a device cannot maintain the information for all IPv6 multicast sources and groups. Therefore, a router might receive IPv6 multicast packets addressed to IPv6 multicast groups that have no members on the local subnet. In this case, the Router-Alert option carried in the IPv6 multicast packets is useful for the router to determine whether to deliver the IPv6 multicast packets to the upper-layer protocol for processing. For more information about the Router-Alert option, see RFC 2113.

An MLD message is processed differently depending on whether it carries the Router-Alert option in the IPv6 header, as follows:

- For compatibility, the device by default ignores the Router-Alert option and processes all received MLD messages, no matter whether the MLD messages carry the Router-Alert option or not.
- To enhance device performance, avoid unnecessary costs, and ensure protocol security, configure the device to discard MLD messages that do not carry the Router-Alert option.

Configuring Router-Alert option handling methods globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD view.	mld	N/A
3. Configure the interface to discard any MLD message without the Router-Alert option.	require-router-alert	By default, the device does not check MLD messages for the Router-Alert option.
4. Enable the insertion of the Router-Alert option into MLD messages.	send-router-alert	By default, MLD messages carry the Router-Alert option.

Configuring Router-Alert option handling methods on an interface

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the interface to discard any MLD message without the Router-Alert option.	mld require-router-alert	By default, the device does not check MLD messages for the Router-Alert option.
4. Enable the insertion of the Router-Alert option into MLD messages.	mld send-router-alert	By default, MLD messages carry the Router-Alert option.

Configuring MLD query and response parameters

On startup, the MLD querier sends MLD general queries at the startup query interval, which is one-quarter of the MLD query interval. The number of queries, or the startup query count, is user configurable.

After startup, the MLD querier periodically sends MLD general queries at the MLD query interval to check for IPv6 multicast group members on the network. You can modify the query interval based on the actual condition of the network.

The MLDv1 querier sends MLD multicast-address-specific queries at the MLD last listener query interval when it receives an MLD done message. The MLDv2 querier sends MLD multicast-address-and-source-specific queries at the MLD last listener query interval when it receives a

multicast group and multicast source mapping change report. The number of queries, or the last listener query count, equals the robustness variable (the maximum number of packet retransmissions).

A multicast listening host starts a timer for each IPv6 multicast group that it has joined when it receives an MLD query (general query, multicast-address-specific query, or multicast-address-and-source-specific query). The timer is initialized to a random value in the range of 0 to the maximum response delay advertised in the MLD query message. When the timer decreases to 0, the host sends an MLD membership report message to the IPv6 multicast group.

To speed up the response of hosts to MLD queries and avoid simultaneous timer expirations causing MLD report traffic bursts, you must properly set the maximum response delay.

- For MLD general queries, the maximum response delay is set by the **max-response-time** command.
- For MLD multicast-address-specific query and multicast-address-and-source-specific query messages, the maximum response delay equals the last listener query interval.

When multiple multicast routers exist on the same subnet, the MLD querier is responsible for sending MLD query messages. If a non-querier router receives no MLD query from the querier when the other querier present interval expires, it considers the querier as having failed and starts a new querier election. Otherwise, the non-querier resets the other querier present timer.

To avoid frequent MLD querier changes, set the other querier present interval greater than the MLD query interval.

To avoid incorrect multicast group member removals, set the MLD query interval greater than the maximum response delay for MLD general queries.

Configuring MLD query and response parameters globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD view.	mld	N/A
3. Configure the MLD querier's robustness variable.	robust-count <i>robust-value</i>	2 times by default. A higher robustness variable makes the MLD querier more robust but results in a longer IPv6 multicast group timeout time.
4. Configure the startup query interval.	startup-query-interval <i>interval</i>	By default, the startup query interval is 1/4 of the "MLD query interval".
5. Configure the startup query count.	startup-query-count <i>value</i>	By default, the startup query count is set to the MLD querier's robustness variable.
6. Configure the MLD query interval.	timer query <i>interval</i>	125 seconds by default.
7. Configure the maximum response delay for MLD general query messages.	max-response-time <i>interval</i>	10 seconds by default.

Step	Command	Remarks
8. Configure the MLD last listener query interval.	last-listener-query-interval <i>interval</i>	1 second by default.
9. Configure the MLD other querier present interval.	timer other-querier-present <i>interval</i>	By default, the other querier present interval is determined by the formula "Other querier present interval (in seconds) = [MLD query interval] × [MLD querier's robustness variable] + [maximum response delay for MLD general query] / 2".

Configuring MLD query and response parameters on an interface

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the MLD querier's robustness variable.	mld robust-count <i>robust-value</i>	2 times by default.
4. Configure the startup query interval.	mld startup-query-interval <i>interval</i>	By default, the startup query interval is 1/4 of the "MLD query interval".
5. Configure the startup query count.	mld startup-query-count <i>value</i>	By default, the startup query count is the same as the robustness variable.
6. Configure the MLD query interval.	mld timer query <i>interval</i>	125 seconds by default.
7. Configure the maximum response delay for MLD general query messages.	mld max-response-time <i>interval</i>	10 seconds by default.
8. Configure the MLD last listener query interval.	mld last-listener-query-interval <i>interval</i>	1 second by default.
9. Configure the MLD other querier present interval.	mld timer other-querier-present <i>interval</i>	By default, the other querier present interval is determined by the formula "Other querier present interval (in seconds) = [MLD query interval] × [MLD querier's robustness variable] + [maximum response delay for MLD general query] / 2".

Configuring MLD fast-leave processing

In some applications, such as ADSL dial-up networking, only one multicast receiver host is attached to a port of the MLD querier. To allow fast response to the MLD done messages of the host when it switches

frequently from one IPv6 multicast group to another, you can enable MLD fast-leave processing on the MLD querier.

With fast-leave processing enabled, after receiving an MLD done message from a host, the MLD querier sends a leave notification to the upstream immediately without first sending MLD multicast-address-specific queries. In this way, the leave latency is reduced on one hand, and the network bandwidth is saved on the other hand.

Configuring MLD fast-leave processing globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD view.	mld	N/A
3. Configure MLD fast-leave processing.	fast-leave [group-policy acl6-number]	Disabled by default.

Configuring MLD fast-leave processing on an interface

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure MLD fast-leave processing.	mld fast-leave [group-policy acl6-number]	Disabled by default.

NOTE:

The MLD fast-leave processing configuration is effective on Layer 3 interfaces other than VLAN interfaces, including Layer 3 Ethernet ports, Layer 3 aggregate interfaces, and Tunnel interfaces.

MLD fast-leave processing is implemented by MLD snooping. For more information about MLD snooping, see "[Configuring MLD snooping](#)."

Enabling the MLD host tracking function

With the MLD host tracking function, the switch can record the information of the member hosts that are receiving IPv6 multicast traffic, including the host IPv6 address, running duration, and timeout time. You can monitor and manage the member hosts according to the recorded information.

Enabling the MLD host tracking function globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD view.	mld	N/A

Step	Command	Remarks
3.	Configure the MLD host tracking function globally. host-tracking	Disabled by default

Enabling the MLD host tracking function on an interface

Step	Command	Remarks
1.	Enter system view. system-view	N/A
2.	Enter interface view. interface <i>interface-type interface-number</i>	N/A
3.	Enable the MLD host tracking function on the interface. mld host-tracking	Disabled by default

Setting the DSCP value for MLD messages

IPv6 uses an eight-bit Traffic class field (called ToS in IPv4) to identify type of service for IP packets. As defined in RFC 2474, the first six bits contains the DSCP priority for prioritizing traffic in the network and the last two bits are reserved.

To set the DSCP value for MLD messages:

Step	Command	Remarks
1.	Enter system view. system-view	N/A
2.	Enter MLD view. mld	N/A
3.	Set the DSCP value for MLD messages. dscp <i>dscp-value</i>	Optional. By default, the DSCP value in MLD messages is 48.

Configuring MLD SSM mapping

Because of some possible restrictions, some receiver hosts on an SSM network might run MLDv1. To provide SSM service support for these receiver hosts, you need to configure the MLD SSM mapping feature on the last hop router.

Configuration prerequisites

Before you configure the MLD SSM mapping feature, complete the following tasks:

- Enable IPv6 forwarding and configure an IPv6 unicast routing protocol so that all devices in the domain can be interoperable at the network layer.
- Configure basic MLD functions.

Enabling MLD SSM mapping

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable the MLD SSM mapping feature.	mld ssm-mapping enable	Disabled by default

NOTE:

To ensure SSM service for all hosts on a subnet, regardless of the MLD version running on the hosts, enable MLDv2 on the interface that forwards IPv6 multicast traffic onto the subnet.

Configuring MLD SSM mappings

By performing this configuration multiple times, you can map an IPv6 multicast group to different IPv6 multicast sources.

If MLDv2 is enabled on a VLAN interface of a switch, and if a port in that VLAN is configured as a simulated host, the simulated host will send MLDv2 reports even if you did not specify an IPv6 multicast source when you configure simulated joining with the **mld-snooping host-join** command. In this case, the corresponding IPv6 multicast group will not be created based on the configured MLD SSM mappings. For more information about the **mld-snooping host-join** command, see *IP Multicast Command Reference*.

To configure an MLD SSM mapping:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter MLD view.	mld	N/A
3. Configure an MLD SSM mapping.	ssm-mapping <i>ipv6-group-address</i> <i>prefix-length</i> <i>ipv6-source-address</i>	No MLD mappings are configured by default.

Configuring MLD proxying

Before you configure the MLD proxying feature, complete the following tasks:

- Enable IPv6 forwarding and configure an IPv6 unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Enable IPv6 multicast routing.

Enabling MLD proxying

You can enable MLD proxying on the interface in the direction toward the root of the multicast forwarding tree to make the device serve as an MLD proxy.

Configuration guidelines

- Each device can have only one interface serving as the MLD proxy interface.
- You cannot enable MLD on interfaces with MLD proxying enabled. Moreover, only the **mld require-router-alert**, **mld send-router-alert**, and **mld version** commands can take effect on such interfaces.
- You cannot enable other IPv6 multicast routing protocols (such as IPv6 PIM-DM or IPv6 PIM-SM) on interfaces with MLD proxying enabled, or vice versa. However, the **source-lifetime**, **source-policy**, and **ssm-policy** commands configured in IPv6 PIM view can still take effect.
- You cannot enable MLD proxying on a VLAN interface with MLD snooping enabled, or vice versa.

Configuration procedure

To enable MLD proxying:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable the MLD proxying feature.	mld proxying enable	Disabled by default

Configuring IPv6 multicast forwarding on a downstream interface

Typically, to avoid duplicate multicast flows, only queriers can forward IPv6 multicast traffic. On MLD proxy devices, a downstream interface must be a querier in order to forward IPv6 multicast traffic to downstream hosts. If the interface has failed in the querier election, you must manually enable IPv6 multicast forwarding on this interface.

ⓘ IMPORTANT:

On a multi-access network with more than one MLD proxy devices, you cannot enable IPv6 multicast forwarding on any other non-querier downstream interface after one of the downstream interfaces of these MLD proxy devices has been elected as the querier. Otherwise, duplicate multicast flows might be received on the multi-access network.

To enable IPv6 multicast forwarding on a downstream interface

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable IPv6 multicast forwarding on a non-querier downstream interface.	mld proxying forwarding	Disabled by default

Displaying and maintaining MLD

△ CAUTION:

The **reset mld group** command might cause multicast data transmission failures.

To display and maintain MLD:

Task	Command	Remarks
Display MLD group information.	display mld group [<i>ipv6-group-address</i> interface <i>interface-type interface-number</i>] [static verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display Layer 2 port information about MLD groups.	display mld group port-info [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display information about the hosts tracked by MLD on an interface.	display mld host interface <i>interface-type interface-number</i> group <i>ipv6-group-address</i> [source <i>ipv6-source-address</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display information about the hosts tracked by MLD on the Layer 2 ports.	display mld host port-info vlan <i>vlan-id</i> group <i>ipv6-group-address</i> [source <i>ipv6-source-address</i>] [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display MLD configuration and running information on the specified interface or all MLD-enabled interfaces.	display mld interface [<i>interface-type interface-number</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the information of the MLD proxying groups.	display mld proxying group [<i>group-address</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.

Task	Command	Remarks
Display the information of the MLD routing table.	display mld routing-table [<i>ipv6-source-address</i> [<i>prefix-length</i>] <i>ipv6-group-address</i> [<i>prefix-length</i>] flags { act suc }] * [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display MLD SSM mappings.	display mld ssm-mapping <i>ipv6-group-address</i> [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display the IPv6 multicast group information created based on the configured MLD SSM mappings.	display mld ssm-mapping group [<i>ipv6-group-address</i> interface <i>interface-type interface-number</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Display information about the hosts that join based on the MLD SSM mappings on an interface.	display mld ssm-mapping host interface <i>interface-type</i> <i>interface-number</i> group <i>ipv6-group-address</i> source <i>ipv6-source-address</i> [{ begin exclude include } <i>regular-expression</i>]	Available in any view.
Remove the dynamic group entries of a specified MLD group or all MLD groups.	reset mld group { all interface <i>interface-type interface-number</i> { all <i>ipv6-group-address</i> [<i>prefix-length</i>] [<i>ipv6-source-address</i> [<i>prefix-length</i>]] } }	Available in user view. This command cannot remove dynamic MLD group entries.
Remove the dynamic Layer 2 port entries of a specified MLD group or all MLD groups.	reset mld group port-info { all <i>ipv6-group-address</i> } [vlan <i>vlan-id</i>]	Available in user view. This command cannot remove the Layer 2 port entries of MLD groups.
Clear MLD SSM mappings.	reset mld ssm-mapping group { all interface <i>interface-type</i> <i>interface-number</i> { all <i>ipv6-group-address</i> [<i>prefix-length</i>] [<i>ipv6-source-address</i> [<i>prefix-length</i>]] } }	Available in user view.

The **display mld host interface** command can display information about the hosts tracked by MLD on Layer 3 interfaces other than VLAN interfaces.

The **display mld ssm-mapping host interface** command can display information about the hosts that join the group based on MLD SSM mappings on Layer 3 interfaces other than VLAN interfaces.

MLD configuration examples

Basic MLD functions configuration example

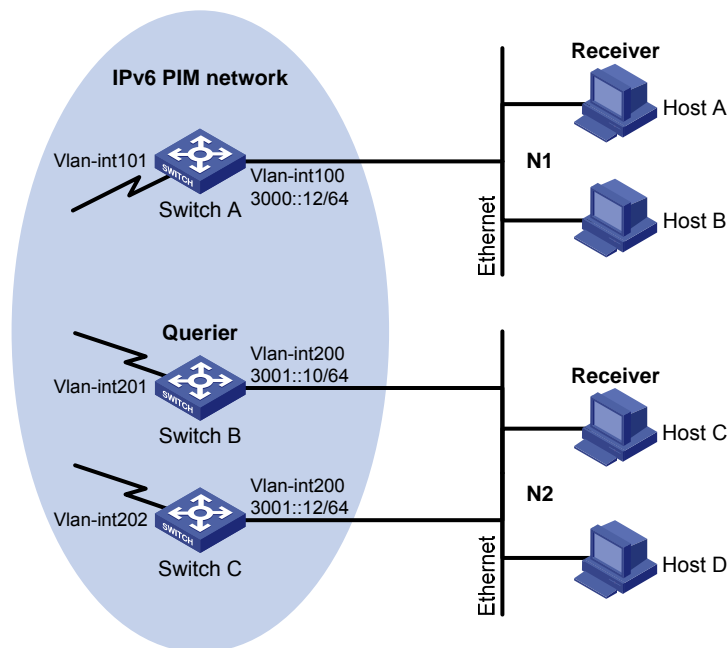
Network requirements

As shown in [Figure 89](#), receivers receive VOD information in the multicast mode. Receivers of different organizations form stub networks N1 and N2, and Host A and Host C are multicast receivers in N1 and N2 respectively.

MLDv1 runs between Switch A and N1. MLDv1 runs between the other two switches (Switch B and Switch C) and N2. Switch B acts as the MLD querier because it has a lower IPv6 address.

The hosts in N1 can join only IPv6 multicast group FF1E::101, and the hosts in N2 can join any IPv6 multicast groups.

Figure 89 Network diagram



Configuration procedure

1. Enable IPv6 forwarding on each switch and configure an IP address and prefix length for each interface as shown in [Figure 89](#). (Details not shown.)
2. Configure OSPFv3 on the switches on the IPv6 PIM network to make sure the switches are interoperable at the network layer and they can dynamically update their routing information. (Details not shown.)
3. Enable the IPv6 multicast routing, MLD and IPv6 PIM-DM:
Enable IPv6 multicast routing on Switch A, enable MLD on VLAN-interface 100, and enable IPv6 PIM-DM on each interface.

```

<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] pim ipv6 dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 dm
[SwitchA-Vlan-interface101] quit

```

Enable IPv6 multicast routing on Switch B, enable MLD on VLAN-interface 200, and enable IPv6 PIM-DM on each interface.

```

<SwitchB> system-view
[SwitchB] multicast ipv6 routing-enable
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] mld enable
[SwitchB-Vlan-interface200] pim ipv6 dm
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 201
[SwitchB-Vlan-interface201] pim ipv6 dm
[SwitchB-Vlan-interface201] quit

```

Enable IPv6 multicast routing on Switch C, enable IPv6 PIM-DM on each interface, and enable MLD on VLAN-interface 200.

```

<SwitchC> system-view
[SwitchC] multicast ipv6 routing-enable
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] mld enable
[SwitchC-Vlan-interface200] pim ipv6 dm
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] pim ipv6 dm
[SwitchC-Vlan-interface202] quit

```

4. Configure an IPv6 multicast group filter on Switch A, so that the hosts connected to VLAN-interface 100 can join IPv6 multicast group FF1E::101 only.

```

[SwitchA] acl ipv6 number 2001
[SwitchA-acl6-basic-2001] rule permit source ff1e::101 128
[SwitchA-acl6-basic-2001] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld group-policy 2001
[SwitchA-Vlan-interface100] quit

```

Verifying the configuration

Display MLD information on VLAN-interface 200 of Switch B.

```

[SwitchB] display mld interface vlan-interface 200
Vlan-interface200(FE80::200:5EFF:FE66:5100):
  MLD is enabled
  Current MLD version is 1
  Value of query interval for MLD(in seconds): 125

```

```

Value of other querier present interval for MLD(in seconds): 255
Value of maximum query response time for MLD(in seconds): 10
Querier for MLD: FE80::200:5EFF:FE66:5100 (this router)
Total 1 MLD Group reported

```

MLD SSM mapping configuration example

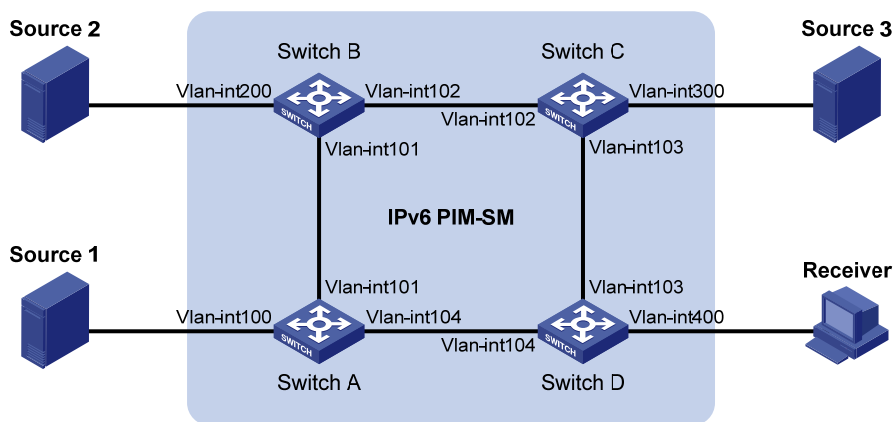
Network requirements

As shown in [Figure 90](#), the IPv6 PIM-SM domain applies both the ASM model and SSM model for IPv6 multicast delivery. Switch D's VLAN-interface 104 serves as the C-BSR and C-RP. The SSM group range is FF3E::/64.

MLDv2 runs on Switch D's VLAN-interface 400. The receiver host runs MLDv1, and does not support MLDv2. Therefore, the Receiver host cannot specify expected multicast sources in its membership reports.

Source 1, Source 2, and Source 3 send IPv6 multicast packets to multicast groups in the IPv6 SSM group range. You can configure the MLD SSM mapping feature on Switch D so that the receiver host will receive IPv6 multicast data from Source 1 and Source 3 only.

Figure 90 Network diagram



Device	Interface	IPv6 address	Device	Interface	IPv6 address
Source 1	—	1001::1/64	Source 3	—	3001::1/64
Source 2	—	2001::1/64	Receiver	—	4001::1/64
Switch A	Vlan-int100	1001::2/64	Switch C	Vlan-int300	3001::2/64
	Vlan-int101	1002::1/64		Vlan-int103	3002::1/64
	Vlan-int104	1003::1/64		Vlan-int102	2002::2/64
Switch B	Vlan-int200	2001::2/64	Switch D	Vlan-int400	4001::2/64
	Vlan-int101	1002::2/64		Vlan-int103	3002::2/64
	Vlan-int102	2002::1/64		Vlan-int104	1003::2/64

Configuration procedure

1. Enable IPv6 forwarding on each switch and configure an IPv6 address and prefix length for each interface as shown in [Figure 90](#). (Details not shown.)

2. Configure OSPFv3 on the switches in the IPv6 PIM-SM domain to make sure the switches are interoperable at the network layer and they can dynamically update their routing information. (Details not shown.)
3. Enable IPv6 multicast routing, enable IPv6 PIM-SM on each interface and enable MLD and MLD SSM mapping on the host-side interface:

Enable IPv6 multicast routing on Switch D, enable IPv6 PIM-SM on each interface, and enable MLD (version 2) and MLD SSM mapping on VLAN-interface 400.

```
<SwitchD> system-view
[SwitchD] multicast ipv6 routing-enable
[SwitchD] interface vlan-interface 400
[SwitchD-Vlan-interface400] mld enable
[SwitchD-Vlan-interface400] mld version 2
[SwitchD-Vlan-interface400] mld ssm-mapping enable
[SwitchD-Vlan-interface400] pim ipv6 sm
[SwitchD-Vlan-interface400] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim ipv6 sm
[SwitchD-Vlan-interface103] quit
[SwitchD] interface vlan-interface 104
[SwitchD-Vlan-interface104] pim ipv6 sm
[SwitchD-Vlan-interface104] quit
```

Enable IPv6 multicast routing on Switch A, and enable IPv6 PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 104
[SwitchA-Vlan-interface104] pim ipv6 sm
[SwitchA-Vlan-interface104] quit
```

Enable IPv6 multicast routing and IPv6 PIM-SM on Switch B and Switch C in the same way. (Details not shown.)

4. Configure C-BSR and C-RP interfaces on Switch D.

```
[SwitchD] pim ipv6
[SwitchD-pim6] c-bsr 1003::2
[SwitchD-pim6] c-rp 1003::2
[SwitchD-pim6] quit
```

5. Configure the IPv6 SSM group range:

Configure the IPv6 SSM group range FF3E::/64 on Switch D.

```
[SwitchD] acl ipv6 number 2000
[SwitchD-acl6-basic-2000] rule permit source ff3e:: 64
[SwitchD-acl6-basic-2000] quit
```

```
[SwitchD] pim ipv6
[SwitchD-pim6] ssm-policy 2000
[SwitchD-pim6] quit
```

Configure the IPv6 SSM group range on Switch A, Switch B and Switch C in the same way.
(Details not shown.)

6. Configure MLD SSM mappings on Switch D.

```
[SwitchD] mld
[SwitchD-mld] ssm-mapping ff3e:: 64 1001::1
[SwitchD-mld] ssm-mapping ff3e:: 64 3001::1
[SwitchD-mld] quit
```

Verifying the configuration

Display MLD SSM mapping information about the IPv6 multicast group FF3E::101 on Switch D.

```
[SwitchD] display mld ssm-mapping ff3e::101
Group: FF3E::101
Source list:
    1001::1
    3001::1
```

Display the IPv6 multicast group information created based on the configured MLD SSM mappings on Switch D.

```
[SwitchD] display mld ssm-mapping group
Total 1 MLD SSM-mapping Group(s).
Interface group report information
Vlan-interface400 (4001::2):
    Total 1 MLD SSM-mapping Group reported
    Group Address: FF3E::101
    Last Reporter: 4001::1
    Uptime: 00:02:04
    Expires: off
```

Display the IPv6 PIM routing table information on Switch D.

```
[SwitchD] display pim ipv6 routing-table
Total 0 (*, G) entry; 2 (S, G) entry

(1001::1, FF3E::101)
    Protocol: pim-ssm, Flag:
    UpTime: 00:13:25
    Upstream interface: Vlan-interface104
        Upstream neighbor: 1003::1
        RPF prime neighbor: 1003::1
    Downstream interface(s) information:
        Total number of downstreams: 1
        1: Vlan-interface400
            Protocol: mld, UpTime: 00:13:25, Expires: -

(3001::1, FF3E::101)
    Protocol: pim-ssm, Flag:
```



```

UpTime: 00:13:25
Upstream interface: Vlan-interface103
  Upstream neighbor: 3002::1
  RPF prime neighbor: 3002::1
Downstream interface(s) information:
  Total number of downstreams: 1
  1: Vlan-interface400
      Protocol: mld, UpTime: 00:13:25, Expires: -

```

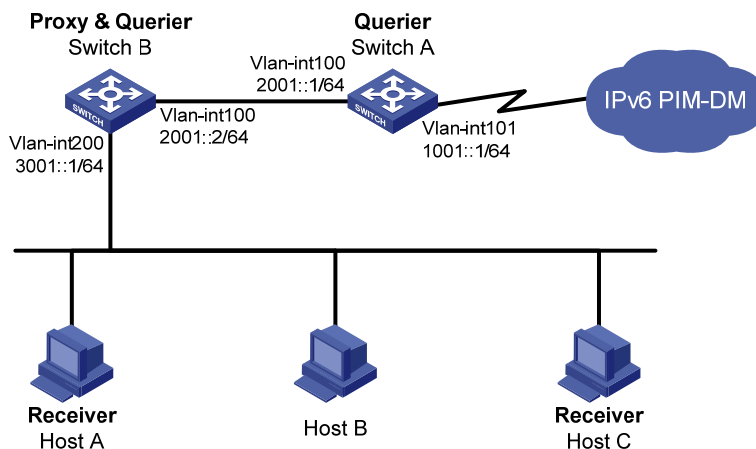
MLD proxying configuration example

Network requirements

As shown in [Figure 91](#), IPv6 PIM-DM runs on the core network. Host A and Host C in the stub network receive VOD information destined to multicast group FF3E::101.

Configure the MLD proxying feature on Switch B so that Switch B can maintain group memberships and forward IPv6 multicast traffic without running IPv6 PIM-DM.

Figure 91 Network diagram



Configuration procedure

1. Enable IPv6 forwarding on each switch and configure the IPv6 address and prefix length of each interface as per [Figure 91](#). (Details not shown.)
2. Enable IPv6 multicast routing, IPv6 PIM-DM, MLD, and MLD proxying:

```
# Enable IPv6 multicast routing on Switch A, IPv6 PIM-DM on VLAN-interface 101, and MLD on
VLAN-interface 100.
```

```

<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 dm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] pim ipv6 dm

```

```
[SwitchA-Vlan-interface100] quit
# Enable IPv6 multicast routing on Switch B, MLD proxying on VLAN-interface 100, and MLD on
VLAN-interface 200.
<SwitchB> system-view
[SwitchB] multicast ipv6 routing-enable
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] mld proxying enable
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] mld enable
[SwitchB-Vlan-interface200] quit
```

Verifying the configuration

```
# Display MLD information on VLAN-interface 100 of Switch B.
[SwitchB] display mld interface vlan-interface 100 verbose
Vlan-interface100(2001::2):
  MLD proxy is enabled
  Current MLD version is 1
  Multicast routing on this interface: enabled
  Require-router-alert: disabled
```

```
# Display MLD group information on Switch A.
[SwitchA] display mld group
Total 1 MLD Group(s).
Interface group report information
Vlan-interface100(2001::1):
  Total 1 MLD Groups reported
  Group Address      Last Reporter      Uptime      Expires
  ff3e::101          2001::2            00:02:04    00:01:15
```

The output shows that the MLD reports sent from the hosts are forwarded to Switch A through the proxy interface, VLAN-interface 100 of Switch B.

Troubleshooting MLD

No member information on the receiver-side router

Symptom

When a host sends a message to announce its joining IPv6 multicast group G, no member information of multicast group G exists on the immediate router.

Analysis

- The correctness of networking and interface connections and whether the protocol layer of the interface is up directly affect the generation of IPv6 group member information.
- IPv6 multicast routing must be enabled on the router and MLD must be enabled on the interface connecting to the host.

- If the MLD version on the router interface is lower than that on the host, the router will not be able to recognize the MLD report from the host.
- If the **mld group-policy** command has been configured on an interface, the interface cannot receive report messages that fail to pass filtering.

Solution

1. Check that the networking, interface connections, and IP address configuration are correct. Check the interface information with the **display mld interface** command. If no information is output, the interface is in an abnormal state. This is usually because you have configured the **shutdown** command on the interface, the interface is not properly connected, or the IPv6 address configuration is not correctly done.
2. Use the **display current-configuration** command to verify that the IPv6 multicast routing is enabled. If not, carry out the **mcast ipv6 routing-enable** command in system view to enable IPv6 multicast routing. In addition, enable MLD on the corresponding interface.
3. You can use the **display mld interface** command to verify that the MLD version on the interface is lower than that on the host.
4. Use the **display current-configuration interface** command to verify that no ACL rule has been configured to restrict the host from joining IPv6 multicast group G. If an IPv6 ACL is configured to restrict the host from joining IPv6 multicast group G, the ACL must be modified to allow IPv6 multicast group G to receive report messages.

Inconsistent memberships on routers on the same subnet

Symptom

Different memberships are maintained on different MLD routers on the same subnet.

Analysis

- A router running MLD maintains multiple parameters for each interface, and these parameters influence one another, forming very complicated relationships. Inconsistent MLD interface parameter configurations for routers on the same subnet will surely result in inconsistent MLD memberships.
- Two MLD versions are available. Although routers running different MLD versions are compatible with hosts, all routers on the same subnet must run the same MLD version. Inconsistent MLD versions running on routers on the same subnet will also lead to inconsistent MLD memberships.

Solution

1. Use the **display current-configuration** command to verify the MLD configuration information on the interface.
2. Use the **display mld interface** command on all routers on the same subnet to check the MLD timers for inconsistent configuration.
3. Use the **display mld interface** command to verify that the routers are running the same MLD version.

Configuring IPv6 PIM (available only on the HP 5500 EI)

Overview

Protocol Independent Multicast for IPv6 (IPv6 PIM) provides IPv6 multicast forwarding by leveraging IPv6 unicast static routes or IPv6 unicast routing tables generated by any IPv6 unicast routing protocol, such as RIPng, OSPFv3, IS-ISv6, or BGP4+. IPv6 PIM uses an IPv6 unicast routing table to perform reverse path forwarding (RPF) check to implement IPv6 multicast forwarding. Independent of the IPv6 unicast routing protocols running on the device, IPv6 multicast routing can be implemented as long as the corresponding IPv6 multicast routing entries are created through IPv6 unicast routes. IPv6 PIM uses the reverse path forwarding (RPF) mechanism to implement IPv6 multicast forwarding. When an IPv6 multicast packet arrives on an interface of the device, RPF check is performed on it. If the RPF check succeeds, the device creates the corresponding routing entry and forwards the packet. If the RPF check fails, the device discards the packet. For more information about RPF, see "[Configuring IPv6 multicast routing and forwarding \(available only on the HP 5500 EI\)](#)."

Based on the implementation mechanism, IPv6 PIM supports the following types:

- Protocol Independent Multicast–Dense Mode for IPv6 (IPv6 PIM-DM)
- Protocol Independent Multicast–Sparse Mode for IPv6 (IPv6 PIM-SM)
- Bidirectional Protocol Independent Multicast for IPv6 (IPv6 BIDIR-PIM)
- Protocol Independent Multicast Source-Specific Multicast for IPv6 (IPv6 PIM-SSM)

To facilitate description, a network comprising IPv6 PIM–supporting routers is referred to as an "IPv6 PIM domain" in this document.

The term "router" in this document refers to both routers and Layer 3 switches.

The term "interface" in this chapter collectively refers to Layer 3 interfaces, including VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

IPv6 PIM-DM overview

IPv6 PIM-DM is a type of dense mode IPv6 multicast protocol. It uses the push mode for IPv6 multicast forwarding, and is suitable for small-sized networks with densely distributed IPv6 multicast members.

The basic implementation of IPv6 PIM-DM is as follows:

- IPv6 PIM-DM assumes that at least one IPv6 multicast group member exists on each subnet of a network. Therefore, IPv6 multicast data is flooded to all nodes on the network. Then, branches without IPv6 multicast forwarding are pruned from the forwarding tree, leaving only those branches that contain receivers. This flood-and-prune process takes place periodically. That is, pruned branches resume IPv6 multicast forwarding when the pruned state times out and then data is flooded again down these branches, and then the branches are pruned again.
- When a new receiver on a previously pruned branch joins an IPv6 multicast group, to reduce the join latency, IPv6 PIM-DM uses the graft mechanism to resume IPv6 multicast data forwarding to that branch.

In general, the IPv6 multicast forwarding path is a source tree. That is, it is a forwarding tree with the IPv6 multicast source as its "root" and IPv6 multicast group members as its "leaves." Because the source tree is the shortest path from the IPv6 multicast source to the receivers, it is also called "shortest path tree (SPT)."

The working mechanism of IPv6 PIM-DM is summarized as follows:

- Neighbor discovery
- SPT establishment
- Graft
- Assert

Neighbor discovery

In an IPv6 PIM domain, a PIM router discovers IPv6 PIM neighbors, maintains IPv6 PIM neighboring relationships with other routers, and builds and maintains SPTs by periodically multicasting IPv6 PIM hello messages to all other IPv6 PIM routers on the local subnet.

NOTE:

Every IPv6 PIM enabled interface on a router sends hello messages periodically and, therefore, learns the IPv6 PIM neighboring information pertinent to the interface.

SPT establishment

The process of constructing an SPT is the flood and prune process.

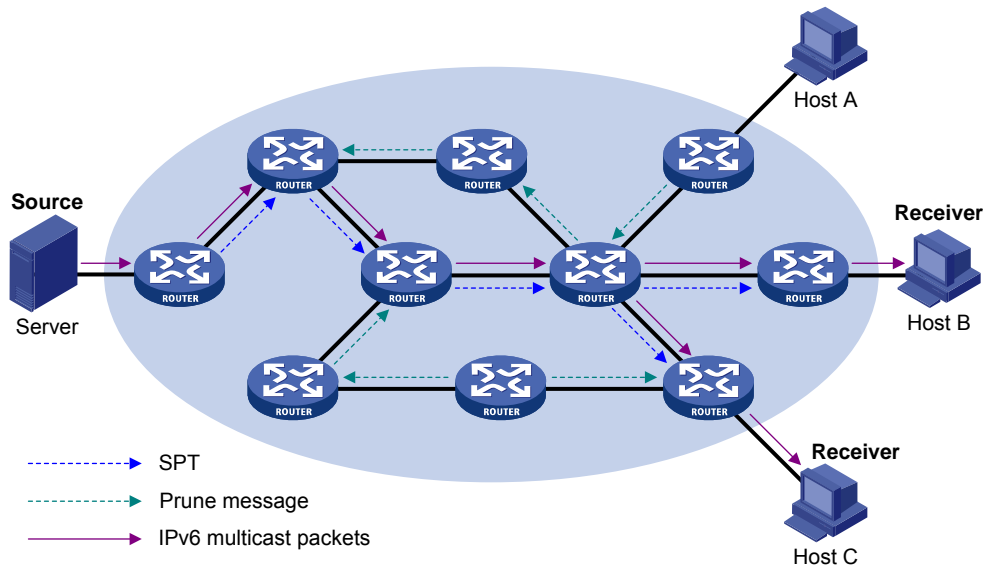
1. In an IPv6 PIM-DM domain, an IPv6 multicast source first floods IPv6 multicast packets when it sends IPv6 multicast data to IPv6 multicast group G . The packet undergoes an RPF check. If the packet passes the RPF check, the router creates an (S, G) entry and forwards the packet to all downstream nodes in the network. In the flooding process, an (S, G) entry is created on all the routers in the IPv6 PIM-DM domain.
2. The nodes without downstream receivers are pruned. A router that has no downstream receivers sends a prune message to the upstream node to notify the upstream node to delete the corresponding interface from the outgoing interface list in the (S, G) entry and stop forwarding subsequent packets addressed to that IPv6 multicast group down to this node.

An (S, G) entry contains the multicast source address S , IPv6 multicast group address G , outgoing interface list, and incoming interface.

For a given IPv6 multicast stream, the interface that receives the IPv6 multicast stream is referred to as "upstream," and the interfaces that forward the IPv6 multicast stream are referred to as "downstream."

A leaf router first initiates a prune process. As shown in Figure 92, a router without any receiver attached to it (the router connected with Host A, for example) sends a prune message, and this prune process continues until only necessary branches remain in the IPv6 PIM-DM domain. These branches constitute the SPT.

Figure 92 SPT establishment in an IPv6 PIM-DM domain



The flood-and-prune process takes place periodically. A pruned state timeout mechanism is provided. A pruned branch restarts multicast forwarding when the pruned state times out and then is pruned again when it no longer has any multicast receiver.

Graft

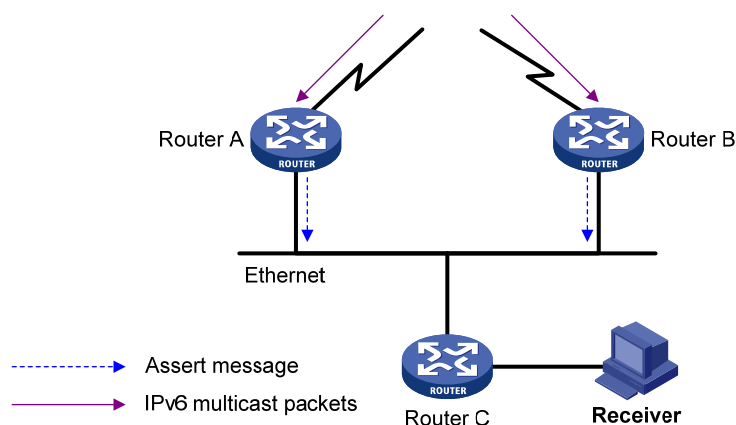
When a host attached to a pruned node joins an IPv6 multicast group, to reduce the join latency, IPv6 PIM-DM uses the graft mechanism to resume IPv6 multicast data forwarding to that branch. The process is as follows:

1. The node that needs to receive IPv6 multicast data sends a graft message toward its upstream node as a request to join the SPT again.
2. After receiving this graft message, the upstream node puts the interface on which the graft was received into the forwarding state and responds with a graft-ack message to the graft sender.
3. If the node that sent a graft message does not receive a graft-ack message from its upstream node, it keeps sending graft messages at a configurable interval until it receives an acknowledgment from its upstream node.

Assert

Where more than one multicast routers exists, the assert mechanism shuts off duplicate IPv6 multicast flows onto the same multi-access network. It does this by electing a unique IPv6 multicast forwarder on the multi-access network.

Figure 93 Assert mechanism



As shown in [Figure 93](#), after Router A and Router B receive an (S, G) IPv6 multicast packet from the upstream node, they both forward the packet to the local subnet. As a result, the downstream node Router C receives two identical multicast packets, and both Router A and Router B, on their own downstream interface, receive a duplicate IPv6 multicast packet that the other has forwarded. After detecting this condition, both routers send an assert message to all IPv6 PIM routers on the local subnet through the downstream interface that received the packet. The assert message contains the multicast source address (S), the multicast group address (G), and the preference and metric of the IPv6 unicast route/IPv6 MBGP route to the source. By comparing these parameters, either Router A or Router B becomes the unique forwarder of the subsequent (S, G) IPv6 multicast packets on the multi-access subnet. The comparison process is as follows:

1. The router with a higher preference to the source wins.
2. If both routers have the same preference to the source, the router with a smaller metric to the source wins.
3. If a tie exists in the route metric to the source, the router with a higher IPv6 link-local address of the downstream interface wins.

IPv6 PIM-SM overview

IPv6 PIM-DM uses the flood-and-prune principle to build SPTs for IPv6 multicast data distribution. Although an SPT has the shortest path, it is built with a low efficiency. Therefore the IPv6 PIM-DM mode is not suitable for large-sized and medium-sized networks.

IPv6 PIM-SM is a type of sparse-mode IPv6 multicast protocol. It uses the pull mode for IPv6 multicast forwarding, and is suitable for large-sized and medium-sized networks with sparsely and widely distributed IPv6 multicast group members.

The basic implementation of IPv6 PIM-SM is as follows:

- IPv6 PIM-SM assumes that no hosts need to receive IPv6 multicast data. In the IPv6 PIM-SM mode, routers must specifically request a particular IPv6 multicast stream before the data is forwarded to them. The core task for IPv6 PIM-SM to implement IPv6 multicast forwarding will build and maintain rendezvous point trees (RPTs). An RPT is rooted at a router in the IPv6 PIM domain as the common node, or rendezvous point (RP), through which the IPv6 multicast data travels along the RPT and reaches the receivers.
- When a receiver is interested in the IPv6 multicast data addressed to a specific IPv6 multicast group, the router connected to this receiver sends a join message to the RP corresponding to that IPv6 multicast group. The path along which the message goes hop by hop to the RP forms a branch of the RPT.
- When an IPv6 multicast source sends IPv6 multicast streams to an IPv6 multicast group, the source-side designated router (DR) first registers the multicast source with the RP by sending register messages to the RP by unicast until it receives a register-stop message from the RP. The arrival of a register message at the RP triggers the establishment of an SPT. The IPv6 multicast source sends subsequent IPv6 multicast packets along the SPT to the RP. After reaching the RP, the IPv6 multicast packet is duplicated and delivered to the receivers along the RPT.

NOTE:

IPv6 multicast traffic is duplicated only where the distribution tree branches, and this process automatically repeats until the IPv6 multicast traffic reaches the receivers.

The working mechanism of IPv6 PIM-SM is summarized as follows:

- Neighbor discovery
- DR election
- RP discovery
- Embedded RP
- RPT establishment
- IPv6 Multicast source registration
- Switchover to SPT
- Assert

Neighbor discovery

IPv6 PIM-SM uses the similar neighbor discovery mechanism as IPv6 PIM-DM does. For more information, see "[Neighbor discovery](#)."

DR election

IPv6 PIM-SM also uses hello messages to elect a DR for a multi-access network (such as a LAN). The elected DR will be the only IPv6 multicast forwarder on this multi-access network.

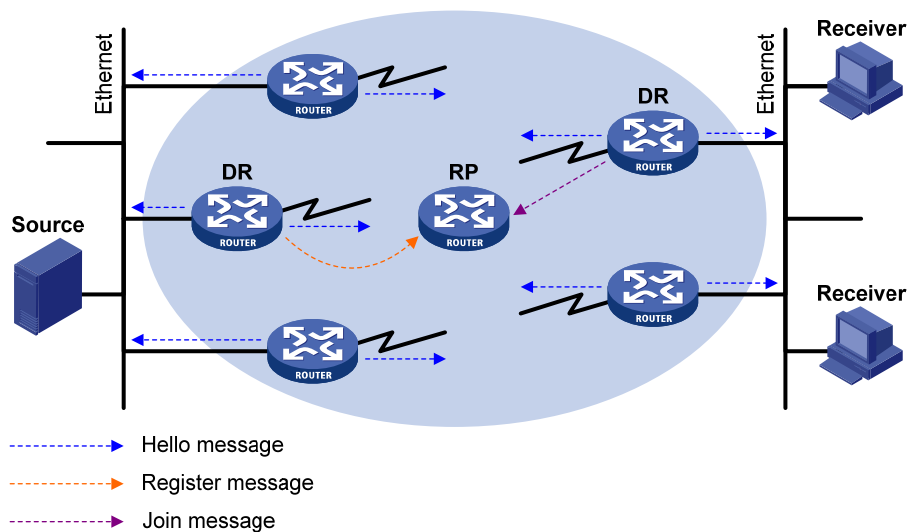
In the case of a multi-access network, a DR must be elected, no matter this network connects to IPv6 multicast sources or to receivers. The DR at the receiver side sends join messages to the RP; the DR at the IPv6 multicast source side sends register messages to the RP.

A DR is elected on a multi-access subnet by means of comparison of the priorities and IPv6 link-local addresses carried in hello messages.

MLD must be enabled on a device that acts as a receiver-side DR before receivers attached to this device can join IPv6 multicast groups through this DR.

For more information about MLD, see "[Configuring MLD \(available only on the HP 5500 EI\)](#)."

Figure 94 DR election



As shown in [Figure 94](#), the DR election process is as follows:

1. Routers on the multi-access network send hello messages to one another. The hello messages contain the router priority for DR election. The router with the highest DR priority will become the DR.
2. In the case of a tie in the router priority, or if any router in the network does not support carrying the DR-election priority in hello messages, the router with the highest IPv6 link-local address will win the DR election.

When the DR works abnormally, a timeout in receiving hello message triggers a new DR election process among the other routers.

RP discovery

The RP is the core of an IPv6 PIM-SM domain. For a small-sized, simple network, one RP is enough for forwarding IPv6 multicast information throughout the network. The position of the RP can be statically specified on each router in the IPv6 PIM-SM domain. In most cases, however, an IPv6 PIM-SM network covers a wide area and a huge amount of IPv6 multicast traffic must be forwarded through the RP. To lessen the RP burden and optimize the topological structure of the RPT, you can configure multiple C-RPs in an IPv6 PIM-SM domain. Among them, an RP is dynamically elected through the bootstrap mechanism. Each elected RP is designated to a different multicast group range. For this purpose, you must configure

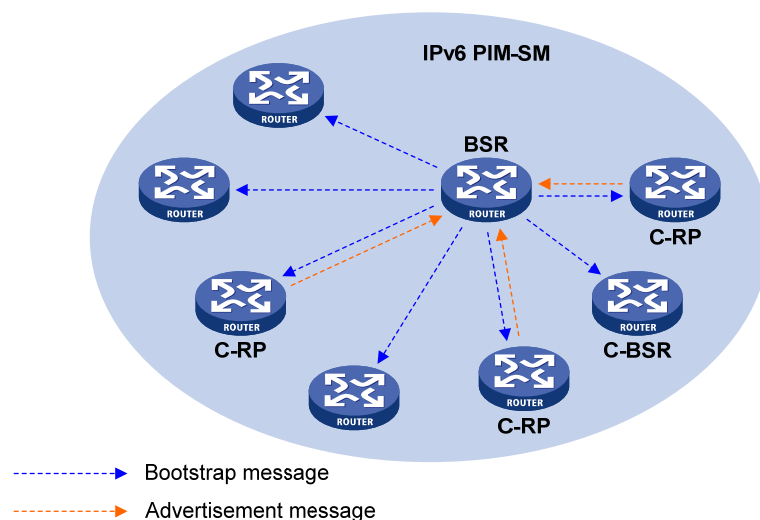
a BSR. The BSR acts as the administrative core of the IPv6 PIM-SM domain. An IPv6 PIM-SM domain can have only one BSR, but can have multiple C-BSRs. If the BSR fails, a new BSR is automatically elected from the C-BSRs to avoid service interruption.

NOTE:

- An RP can provide services for multiple IPv6 multicast groups, but an IPv6 multicast group only uses one RP.
- A device can act as a C-RP and a C-BSR at the same time.

As shown in Figure 95, each C-RP periodically unicasts its advertisement messages (C-RP-Adv messages) to the BSR. An advertisement message contains the address of the advertising C-RP and the IPv6 multicast group range to which it is designated. The BSR collects these advertisement messages and organizes the C-RP information into an RP-set, which is a database of mappings between IPv6 multicast groups and RPs. The BSR then encapsulates the RP-set in the bootstrap messages (BSMs) and floods the bootstrap messages to the entire IPv6 PIM-SM domain.

Figure 95 BSR and C-RPs



Based on the information in the RP-set, all routers in the network can select the proper RP for a specific IPv6 multicast group based on the following rules:

1. The C-RP that is designated to the smallest IPv6 multicast group range wins.
2. If all the C-RPs are designated to the same IPv6 multicast group range, the C-RP with the highest priority wins.
3. If all the C-RPs are designated to the same IPv6 multicast group range and have the same priority, the C-RP with the largest hash value (calculated through the hashing algorithm) wins.
4. If all the C-RPs are designated to the same IPv6 multicast group range and have the same priority and hash value, the C-RP that has the highest IPv6 address wins.

The hashing algorithm used for RP calculation is "Value (G, M, C_i) = (1103515245 * ((1103515245 * (G & M) + 12345) XOR C_i) + 12345) mod 2³¹."

Table 11 Values in the hashing algorithm

Value	Description
Value	Hash value.
G	The digest from the exclusive-or (XOR) operation between the 32-bit segments of the IPv6 multicast group address. For example, if the IPv6 multicast address is FF0E:C20:1A3:63::101, $G = 0xFF0E0C20 \text{ XOR } 0x01A30063 \text{ XOR } 0x00000000 \text{ XOR } 0x00000101$.
M	Hash mask length.
C_i	The digest from the exclusive-or (XOR) operation between the 32-bit segments of the C-RP IPv6 address. For example, if the IPv6 address of the C-RP is 3FFE:B00:C18:1::10, $C_i = 0x3FFE0B00 \text{ XOR } 0x0C180001 \text{ XOR } 0x00000000 \text{ XOR } 0x00000010$.
&	Logical operator of "and."
XOR	Logical operator of "exclusive-or."
mod	Modulo operator, which gives the remainder of an integer division.

Embedded RP

The embedded RP mechanism enables a router to resolve the RP address from an IPv6 multicast address so that the IPv6 multicast group is mapped to an RP. This RP can take the place of the statically configured RP or the RP dynamically calculated based on the BSR mechanism. The DR does not need to identify the RP address beforehand. The specific process is as follows.

At the receiver side, the following occur:

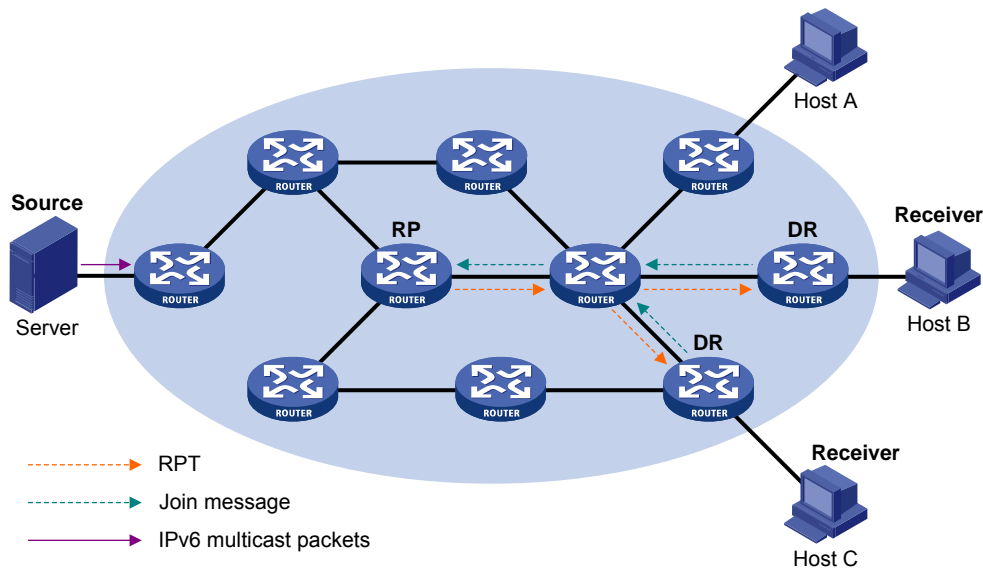
1. A receiver host initiates an MLD report to announce that it is joining an IPv6 multicast group.
2. After receiving the MLD report, the receiver-side DR resolves the RP address embedded in the IPv6 multicast address and sends a join message to the RP.

At the IPv6 multicast source side, the following occur:

1. The IPv6 multicast source sends IPv6 multicast traffic to the IPv6 multicast group.
2. The source-side DR resolves the RP address embedded in the IPv6 multicast address, and sends a register message to the RP.

RPT establishment

Figure 96 RPT establishment in an IPv6 PIM-SM domain



As shown in [Figure 96](#), the process of building an RPT is as follows:

1. When a receiver joins IPv6 multicast group G , it uses an MLD report message to inform the directly connected DR.
2. After getting the IPv6 multicast group G 's receiver information, the DR sends a join message, which is forwarded hop by hop to the RP that corresponds to the multicast group.
3. The routers along the path from the DR to the RP form an RPT branch. Each router on this branch generates a $(*, G)$ entry in its forwarding table. The asterisk means any IPv6 multicast source. The RP is the root of the RPT, and the DRs are the leaves of the RPT.

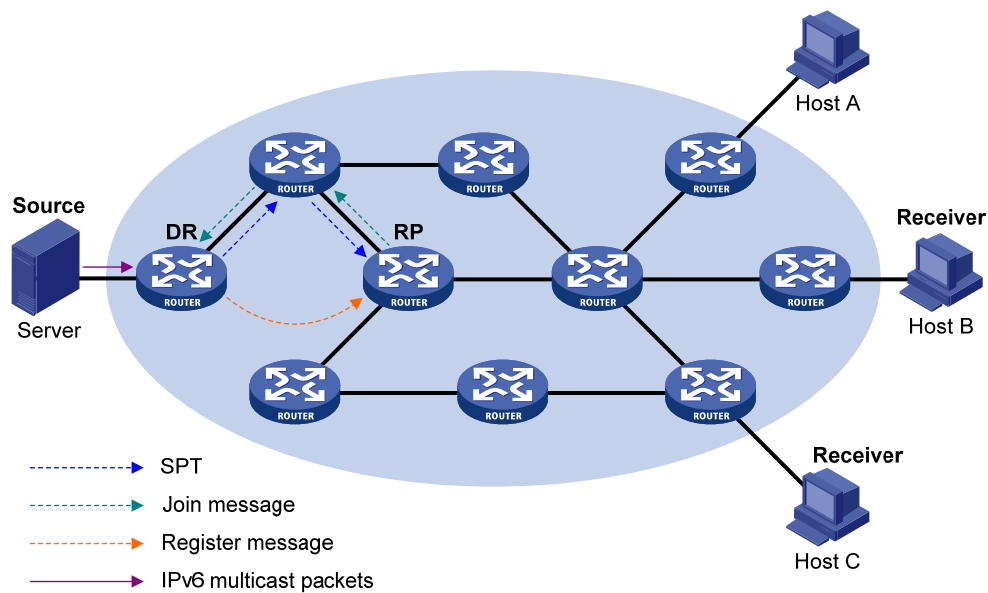
The IPv6 multicast data addressed to the IPv6 multicast group G flows through the RP, reaches the corresponding DR along the established RPT, and finally is delivered to the receiver.

When a receiver is no longer interested in the IPv6 multicast data addressed to a multicast group G , the directly connected DR sends a prune message, which goes hop by hop along the RPT to the RP. After receiving the prune message, the upstream node deletes the interface connected with this downstream node from the outgoing interface list and determines whether it has receivers for that IPv6 multicast group. If not, the router continues to forward the prune message to its upstream router.

Multicast source registration

The purpose of IPv6 multicast source registration will inform the RP about the existence of the IPv6 multicast source.

Figure 97 IPv6 multicast source registration



As shown in Figure 97, the IPv6 multicast source registers with the RP as follows:

1. The IPv6 multicast source S sends the first IPv6 multicast packet to IPv6 multicast group G. After receiving the multicast packet, the DR that directly connects to the multicast source encapsulates the packet in a register message. Then it sends the message to the corresponding RP by unicast.
2. When the RP receives the register message, it extracts the multicast packet from the register message and forwards the multicast IPv6 multicast packet down the RPT, and sends an (S, G) join message hop by hop toward the IPv6 multicast source. The routers along the path from the RP to the IPv6 multicast source form an SPT branch. Each router on this branch generates an (S, G) entry in its forwarding table. The source-side DR is the root of the SPT, and the RP is the leaf of the SPT.
3. The subsequent IPv6 multicast data from the IPv6 multicast source travels along the established SPT to the RP, and then the RP forwards the data along the RPT to the receivers. When the IPv6 multicast traffic arrives at the RP along the SPT, the RP sends a register-stop message to the source-side DR by unicast to stop the source registration process.

NOTE:

The RP is configured to initiate a switchover to SPT as described in this section. Otherwise, the DR at the IPv6 multicast source side keeps encapsulating multicast data in register messages and the registration process will not stop unless no outgoing interfaces exist in the (S, G) entry on the RP.

Switchover to SPT

In an IPv6 PIM-SM domain, an IPv6 multicast group corresponds to one RP and one RPT. Before the switchover to SPT occurs, the DR at the IPv6 multicast source side encapsulates all multicast data destined to the multicast group in register messages and sends these messages to the RP. After receiving these register messages, the RP extracts the multicast data and sends the multicast data down the RPT to the

DRs at the receiver side. The RP acts as a transfer station for all IPv6 multicast packets. The whole process involves the following issues:

- The DR at the source side and the RP need to implement complicated encapsulation and de-encapsulation of IPv6 multicast packets.
- IPv6 multicast packets are delivered along a path that might not be the shortest one.
- An increase in IPv6 multicast traffic heavily burdens the RP, increasing the risk of failure.

To solve the issues, IPv6 PIM-SM allows an RP or the DR at the receiver side to initiate a switchover to SPT:

1. The RP initiates a switchover to SPT.

The RP can periodically check the passing-by IPv6 multicast packets. If it finds that the traffic rate exceeds a configurable threshold, the RP sends an (S, G) join message hop by hop toward the IPv6 multicast source to establish an SPT between the DR at the source side and the RP. Subsequent IPv6 multicast data travels along the established SPT to the RP.

For more information about the switchover to SPT initiated by the RP, see "[Multicast source registration](#)."

2. The receiver-side DR initiates a switchover to SPT

After receiving the first IPv6 multicast packet, the receiver-side DR initiates an SPT switchover process, as follows:

- The receiver-side DR sends an (S, G) join message hop by hop toward the IPv6 multicast source. When the join message reaches the source-side DR, all the routers on the path have installed the (S, G) entry in their forwarding table, and thus an SPT branch is established.
- When the IPv6 multicast packets travel to the router where the RPT and the SPT deviate, the router drops the multicast packets received from the RPT and sends an RP-bit prune message hop by hop to the RP. After receiving this prune message, the RP sends a prune message toward the IPv6 multicast source (supposing only one receiver exists) to implement SPT switchover.
- IPv6 multicast data is directly sent from the source to the receivers along the SPT.

IPv6 PIM-SM builds SPTs through SPT switchover more economically than IPv6 PIM-DM does through the flood-and-prune mechanism.

Assert

IPv6 PIM-SM uses a similar assert mechanism as IPv6 PIM-DM does. For more information, see "[Assert](#)."

IPv6 BIDIR-PIM overview

In some many-to-many applications, such as multi-side video conference, there might be multiple receivers interested in multiple IPv6 multicast sources simultaneously. With IPv6 PIM-DM or IPv6 PIM-SM, each router along the SPT must create an (S, G) entry for each IPv6 multicast source, consuming a lot of system resources. IPv6 BIDIR-PIM is introduced to address this problem. Derived from IPv6 PIM-SM, IPv6 BIDIR-PIM builds and maintains bidirectional RPTs, each of which is rooted at an RP and connects IPv6 multiple multicast sources with multiple receivers. Traffic from the IPv6 multicast sources is forwarded

through the RP to the receivers along the bidirectional RPT. In this case, each router needs to maintain only a (*, G) multicast routing entry, saving system resources.

IPv6 BIDIR-PIM is suitable for networks with dense multicast sources and dense receivers.

The working mechanism of IPv6 BIDIR-PIM is summarized as follows:

- Neighbor discovery
- RP discovery
- DF election
- Bidirectional RPT building

Neighbor discovery

IPv6 BIDIR-PIM uses the same neighbor discovery mechanism as IPv6 PIM-SM does. For more information, see "[Neighbor discovery](#)."

RP discovery

IPv6 BIDIR-PIM uses the same RP discovery mechanism as IPv6 PIM-SM does. For more information, see "[RP discovery](#)."

In IPv6 PIM-SM, an RP must be specified with a real IPv6 address. In IPv6 BIDIR-PIM, however, an RP can be specified with a virtual IPv6 address, which is called the rendezvous point address (RPA). The link corresponding to the RPA's subnet is called the rendezvous point link (RPL). All interfaces connected to the RPL can act as RPs, which back up one another.

In IPv6 BIDIR-PIM, an RPF interface is the interface pointing to an RP, and an RPF neighbor is the address of the next hop to the RP.

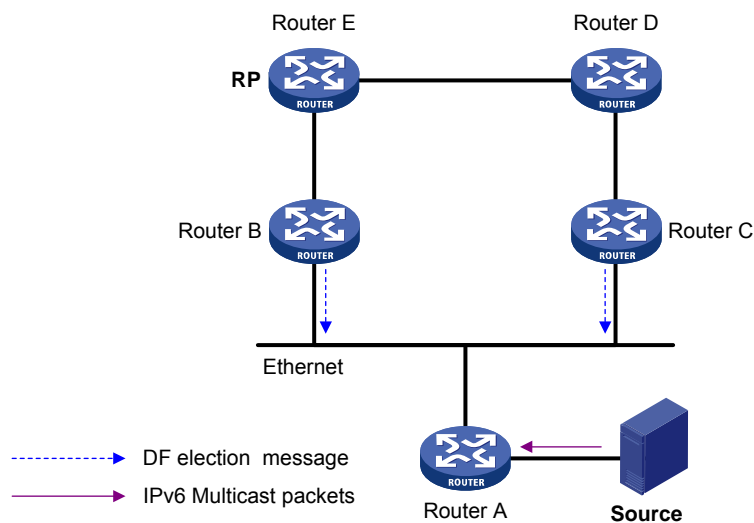
DF election

On a network segment with multiple multicast routers, the same multicast packets might be forwarded to the RP repeatedly. To address this issue, IPv6 BIDIR-PIM uses a DF election mechanism to elect a unique designated forwarder (DF) for each RP on every network segment within the IPv6 BIDIR-PIM domain, and allows only the DF to forward multicast data to the RP.

NOTE:

DF election is not necessary for an RPL.

Figure 98 DF election



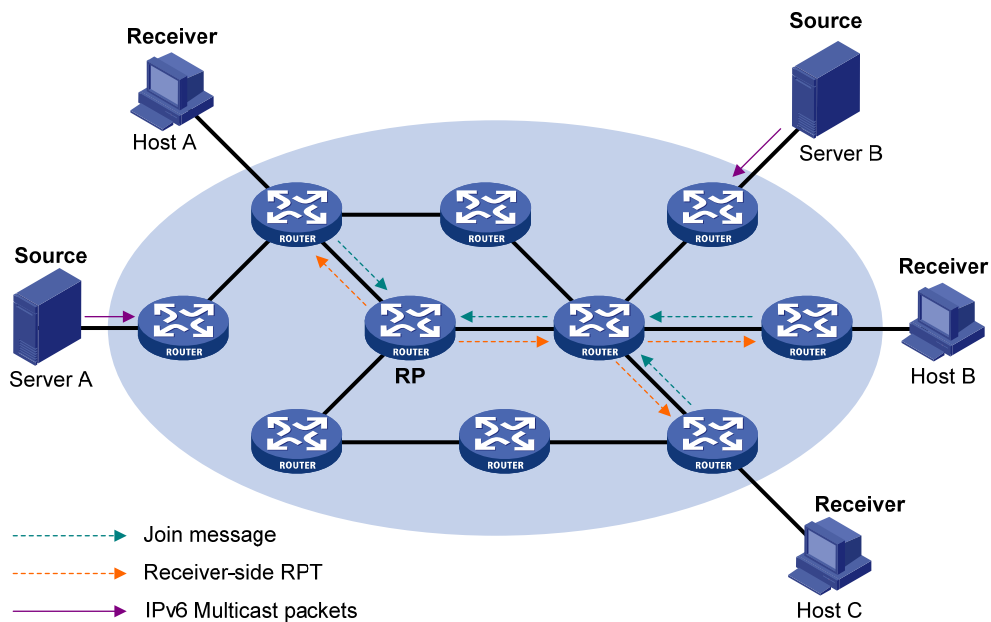
As shown in Figure 98, without the DF election mechanism, both Router B and Router C can receive multicast packets from Router A, and they might both forward the packets to downstream routers on the local subnet. As a result, the RP (Router E) receives duplicate multicast packets. With the DF election mechanism, once receiving the RP information, Router B and Router C initiate a DF election process for the RP:

1. Router B and Router C multicast DF election messages to all IPv6 PIM routers. The election messages carry the RP's address, and the priority and metric of the IPv6 unicast route or IPv6 MBGP route to the RP.
2. The router with a route of the highest priority becomes the DF.
3. In the case of a tie, the router with the route with the lowest metric wins the DF election.
4. In the case of a tie in the metric, the router with the highest link-local IPv6 address wins.

Bidirectional RPT building

A bidirectional RPT comprises a receiver-side RPT and a source-side RPT. The receiver-side RPT is rooted at the RP and takes the routers directly connected with the receivers as leaves. The source-side RPT is also rooted at the RP but takes the routers directly connected with the IPv6 multicast sources as leaves. The processes for building these two parts are different.

Figure 99 RPT building at the receiver side

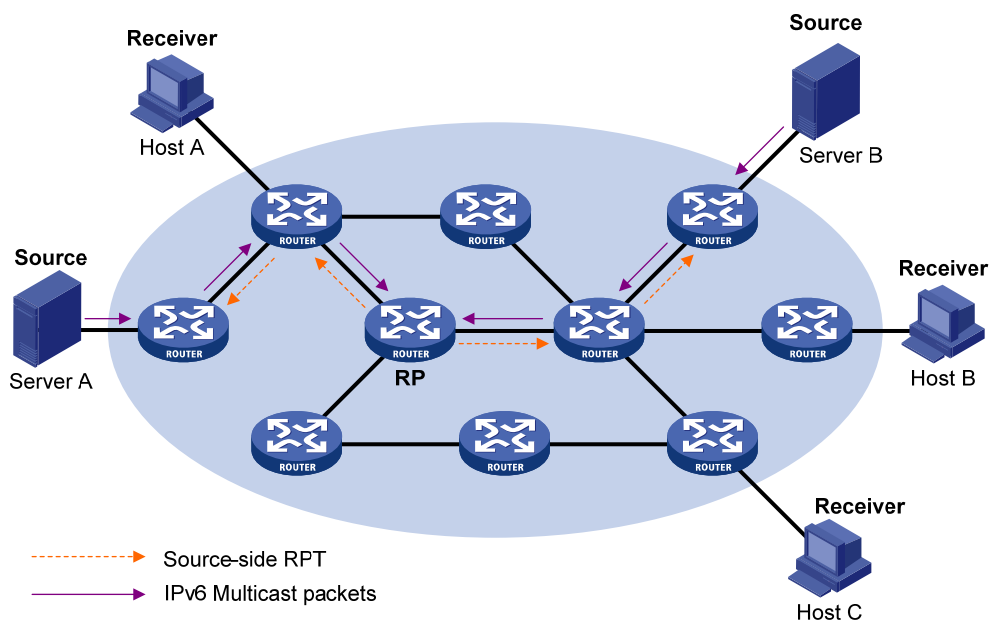


As shown in [Figure 99](#), the process for building a receiver-side RPT is similar to that for building an RPT in IPv6 PIM-SM:

1. When a receiver joins IPv6 multicast group G , it uses an MLD message to inform the directly connected router.
2. After getting the receiver information, the router sends a join message, which is forwarded hop by hop to the RP of the IPv6 multicast group.
3. The routers along the path from the receiver's directly connected router to the RP form an RPT branch, and each router on this branch adds a $(*, G)$ entry to its forwarding table. The $*$ means any IPv6 multicast source.

When a receiver is no longer interested in the multicast data addressed to IPv6 multicast group G , the directly connected router sends a prune message, which goes hop by hop along the reverse direction of the RPT to the RP. After receiving the prune message, each upstream node deletes the interface connected with the downstream node from the outgoing interface list and checks whether it has receivers in that IPv6 multicast group. If not, the router continues to forward the prune message to its upstream router.

Figure 100 RPT building at the multicast source side



As shown in Figure 100, the process of building a source-side RPT is relatively simple:

1. When an IPv6 multicast source sends IPv6 multicast packets to IPv6 multicast group G, the DF in each network segment unconditionally forwards the packets to the RP.
2. The routers along the path from the source's directly connected router to the RP form an RPT branch. Each router on this branch adds a (*, G) entry to its forwarding table. The * means any IPv6 multicast source.

After a bidirectional RPT is built, multicast traffic is forwarded along the source-side RPT and receiver-side RPT from IPv6 multicast sources to receivers.

NOTE:

If a receiver and an IPv6 multicast source are at the same side of the RP, the source-side RPT and the receiver-side RPT might meet at a node before reaching the RP. In this case, IPv6 multicast packets from the IPv6 multicast source to the receiver are directly forwarded by the node to the receiver, instead of by the RP.

IPv6 administrative scoping overview

Division of IPv6 PIM-SM domains

Typically, an IPv6 PIM-SM/IPv6 BIDIR-PIM domain contains only one BSR, which is responsible for advertising RP-set information within the entire IPv6 PIM-SM/IPv6 BIDIR-PIM domain. The information for all multicast groups is forwarded within the network scope administered by the BSR. We call this IPv6 non-scoped BSR mechanism.

To implement refined management, an IPv6 PIM-SM/IPv6 BIDIR-PIM domain can be divided into one IPv6 global scope zone and multiple IPv6 administratively scoped zones (IPv6 admin-scope zones). We call this IPv6 administrative scoping mechanism.

The IPv6 administrative scoping mechanism effectively releases stress on the management in a single-BSR domain and enables provision of zone-specific services using private group addresses.

IPv6 admin-scope zones correspond to IPv6 multicast groups with different scope values in their group addresses. The boundary of the IPv6 admin-scope zone is formed by zone border routers (ZBRs). Each IPv6 admin-scope zone maintains one BSR, which provides services for multicast groups within a specific scope. IPv6 multicast protocol packets, such as assert messages and bootstrap messages, for a specific group range cannot cross the IPv6 admin-scope zone boundary. IPv6 multicast group ranges to which different IPv6 admin-scope zones are designated can overlap. An IPv6 multicast group is valid only within its local IPv6 admin-scope zone, functioning as a private group address.

The IPv6 global scope zone maintains a BSR, which provides services for the IPv6 multicast groups with the Scope field in their group addresses being 14.

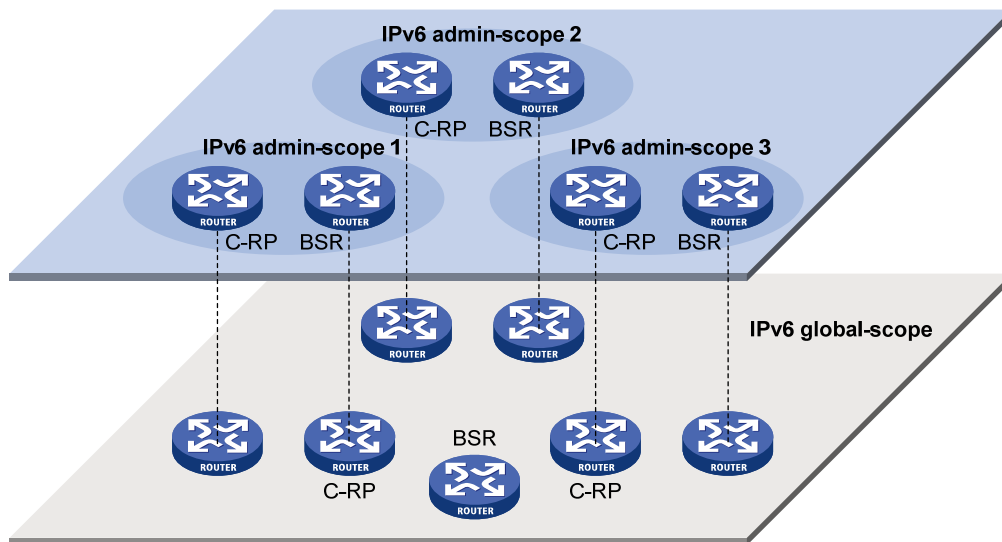
Relationship between IPv6 admin-scope zones and the IPv6 global scope zone

The IPv6 global scope zone and each IPv6 admin-scope zone have their own C-RPs and BSRs. These devices are effective only to their respective zones, and the BSR election and the RP election are implemented independently. Each IPv6 admin-scoped zone has its own boundary. The IPv6 multicast information within a zone cannot cross this boundary in either direction. You can have a better understanding of the IPv6 global-scoped zone and IPv6 admin-scoped zones based on geographical locations and the scope field values.

- In view of geographical locations

An IPv6 admin-scope zone is a logical zone for particular IPv6 multicast groups with the same scope field value. The IPv6 multicast packets for such IPv6 multicast groups are confined within the local IPv6 admin-scope zone and cannot cross the boundary of the zone.

Figure 101 Relationship in view of geographical locations

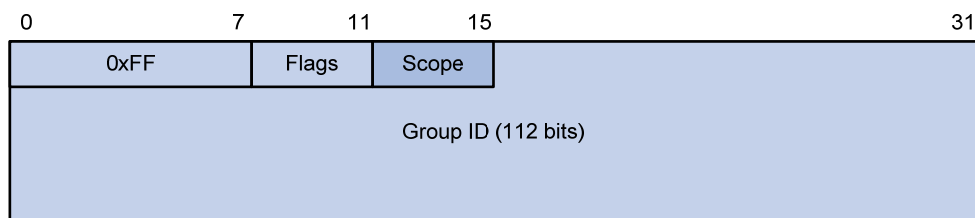


As shown in [Figure 101](#), for the IPv6 multicast groups with the same scope field value, the IPv6 admin-scope zones must be geographically separated and isolated. The IPv6 global-scope zone includes all routers in the IPv6 PIM-SM domain or IPv6 BIDIR-PIM domain. IPv6 multicast packets that do not belong to any IPv6 admin-scope zones are forwarded in the entire IPv6 PIM-SM domain or IPv6 BIDIR-PIM domain.

- In view of the scope field values

In terms of the scope field values, the scope field in an IPv6 multicast group address shows which zone the IPv6 multicast group belongs to.

Figure 102 IPv6 multicast address format



An IPv6 admin-scope zone with a larger scope field value contains an IPv6 admin-scope zone with a smaller scope field value. The zone with the scope field value of E is the IPv6 global-scope zone. [Table 2](#) lists the possible values of the scope field.

Table 2 Values of the Scope field

Value	Meaning	Remarks
0, F	Reserved	N/A
1	Interface-local scope	N/A
2	Link-local scope	N/A

Value	Meaning	Remarks
3	Subnet-local scope	IPv6 admin-scope zone
4	Admin-local scope	IPv6 admin-scope zone
5	Site-local scope	IPv6 admin-scope zone
6, 7, 9 through D	Unassigned	IPv6 admin-scope zone
8	Organization-local scope	IPv6 admin-scope zone
E	Global scope	IPv6 global-scope zone

IPv6 PIM-SSM overview

The source-specific multicast (SSM) model and the any-source multicast (ASM) model are opposites. The ASM model includes the IPv6 PIM-DM and IPv6 PIM-SM modes. You can implement the SSM model by leveraging part of the IPv6 PIM-SM technique. It is also called "IPv6 PIM-SSM."

The SSM model provides a solution for source-specific multicast. It maintains the relationships between hosts and routers through MLDv2.

In actual application, MLDv2 and part of IPv6 PIM-SM technique is adopted to implement the SSM model. In the SSM model, receivers know exactly where an IPv6 multicast source is located by using advertisements, consultancy, and so on. This model does not require RP or RPT, and it does not require a source registration process for the purpose of discovering IPv6 multicast sources in other IPv6 PIM domains.

In IPv6 PIM-SSM, the term "channel " refers to an IPv6 multicast group, and the term "channel subscription" refers to a join message.

The working mechanism of IPv6 PIM-SSM is summarized as follows:

- Neighbor discovery
- DR election
- SPT building

Neighbor discovery

IPv6 PIM-SSM uses the same neighbor discovery mechanism as in IPv6 PIM-SM. For more information, see "[Neighbor discovery](#)."

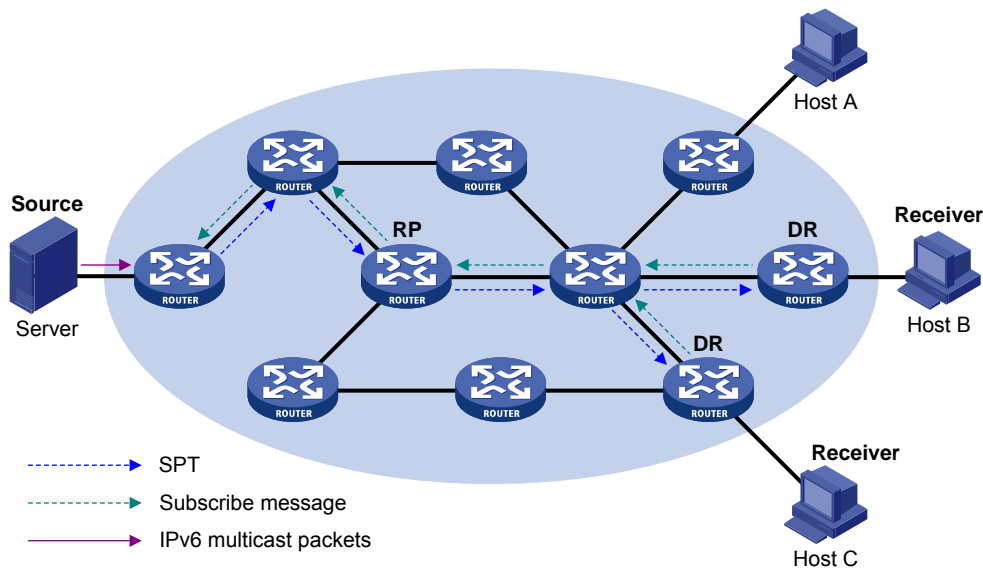
DR election

IPv6 PIM-SSM uses the same DR election mechanism as in IPv6 PIM-SM. For more information, see "[DR election](#)."

SPT building

The decision to build an RPT for IPv6 PIM-SM or an SPT for IPv6 PIM-SSM depends on whether the IPv6 multicast group that the receiver will join falls into the IPv6 SSM group range. The IPv6 SSM group range that IANA has reserved is FF3x::/32, where x represents any legal address scope.

Figure 103 Building an SPT in IPv6 PIM-SSM



As shown in [Figure 103](#), Hosts B and C are IPv6 multicast information receivers. They send an MLDv2 report message to the respective DRs to announce that they are interested in the information about the specific IPv6 multicast source S and that sent to the IPv6 multicast group G.

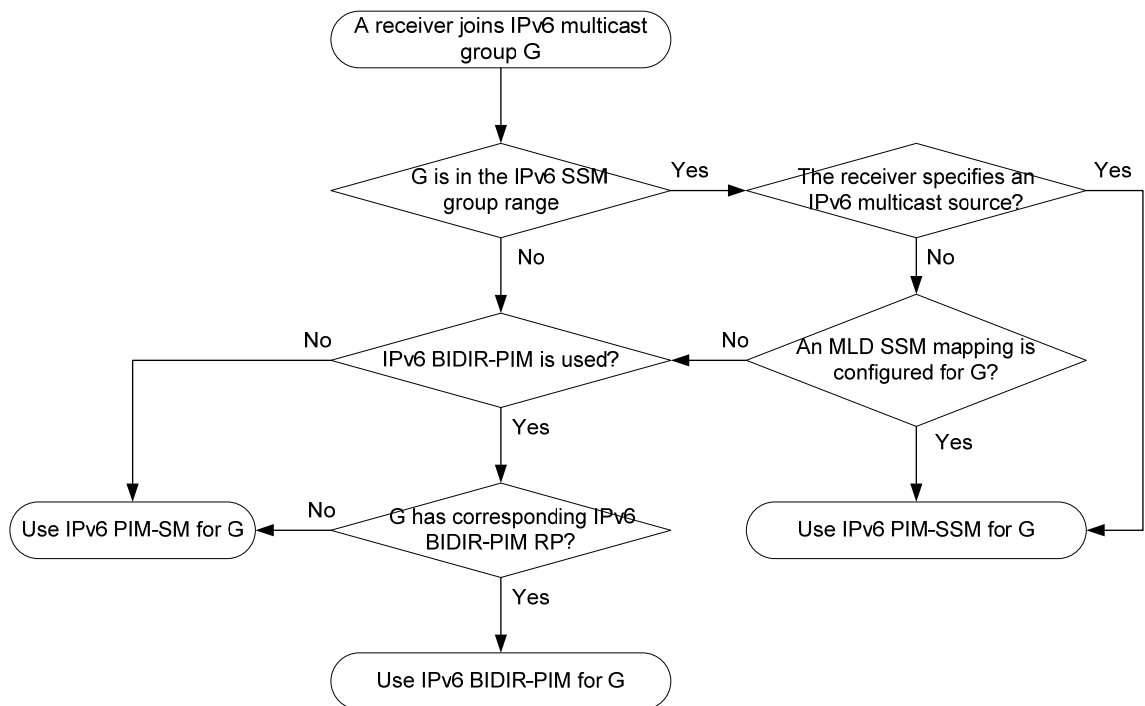
The DR that has received the report first determines whether the IPv6 group address in this message falls into the IPv6 SSM group range and then does the following:

- If the IPv6 group address in the message does fall into the IPv6 SSM group range, the IPv6 PIM-SSM model is built. The DR sends a channel subscription message hop by hop toward the IPv6 multicast source S. An (S, G) entry is created on all routers on the path from the DR to the source. Thus, an SPT is built in the network, with the source S as its root and receivers as its leaves. This SPT is the transmission channel in IPv6 PIM-SSM.
- If the IPv6 group address in the message does not fall into the IPv6 SSM group range, the DR follows the IPv6 PIM-SM process. The receiver-side DR sends a (*, G) join message to the RP, and the source-side DR registers the IPv6 multicast source.

Relationship among IPv6 PIM protocols

In an IPv6 PIM network, IPv6 PIM-DM cannot work with IPv6 PIM-SM, IPv6 BIDIR-PIM, or IPv6 PIM-SSM. However, IPv6 PIM-SM, IPv6 BIDIR-PIM, and IPv6 PIM-SSM can work together. When they work together, which one is chosen for a receiver trying to join a group depends, as shown in [Figure 104](#).

Figure 104 Relationship among IPv6 PIM protocols



For more information about MLD SSM mapping, see "[Configuring MLD \(available only on the HP 5500 EI\)](#)."

Protocols and standards

- RFC 3973, *Protocol Independent Multicast-Dense Mode(PIM-DM):Protocol Specification(Revised)*
- RFC 4601, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)*
- RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*
- RFC 5015, *Bidirectional Protocol Independent Multicast (BIDIR-PIM)*
- RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*
- RFC 4607, *Source-Specific Multicast for IP*
- draft-ietf-ssm-overview-05, *An Overview of Source-Specific Multicast (SSM)*

Configuring IPv6 PIM-DM

IPv6 PIM-DM configuration task list

Task	Remarks
Enabling IPv6 PIM-DM	Required
Enabling state-refresh capability	Optional

Task	Remarks
Configuring state refresh parameters	Optional
Configuring IPv6 PIM-DM graft retry period	Optional
Configuring IPv6 PIM common features	Optional

Configuration prerequisites

Before you configure IPv6 PIM-DM, complete the following tasks:

- Enable IPv6 forwarding and configure an IPv6 unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Determine the interval between state refresh messages.
- Determine the minimum time to wait before receiving a new refresh message.
- Determine the hop limit value of state-refresh messages.
- Determine the graft retry period.

Enabling IPv6 PIM-DM

With IPv6 PIM-DM enabled, a router sends hello messages periodically to discover IPv6 PIM neighbors and processes messages from the IPv6 PIM neighbors. When you deploy an IPv6 PIM-DM domain, enable IPv6 PIM-DM on all non-border interfaces of routers.

ⓘ IMPORTANT:

- All the interfaces of the same device must operate in the same IPv6 PIM mode.
- IPv6 PIM-DM cannot be used for IPv6 multicast groups in the IPv6 SSM group range.

To enable IPv6 PIM-DM:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IPv6 multicast routing.	multicast ipv6 routing-enable	Disabled by default.
3. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable IPv6 PIM-DM.	pim ipv6 dm	Disabled by default.

Enabling state-refresh capability

Pruned interfaces resume multicast forwarding when the pruned state times out. To prevent this, the router directly connected with the IPv6 multicast source periodically sends an (S, G) state-refresh message, which is forwarded hop by hop along the initial flooding path of the IPv6 PIM-DM domain, to refresh the

prune timer state of all the routers on the path. A multi-access subnet can have the state-refresh capability only if the state-refresh capability is enabled on all IPv6 PIM routers on the subnet.

To enable the state-refresh capability:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable the state-refresh capability.	pim ipv6 state-refresh-capable	Optional. Enabled by default.

Configuring state refresh parameters

The router directly connected with the multicast source periodically sends state-refresh messages. You can configure the interval for sending such messages.

A router might receive multiple state-refresh messages within a short time. Some messages might be duplicated messages. To keep a router from receiving such duplicated messages, you can configure the time that the router must wait before receiving the next state-refresh message. If the router receives a new state-refresh message within the waiting time, it discards it. If this timer times out, the router will accept a new state-refresh message, refresh its own IPv6 PIM-DM state, and reset the waiting timer.

The hop limit value of a state-refresh message decrements by 1 whenever it passes a router before it is forwarded to the downstream node until the hop limit value comes down to 0. In a small network, a state-refresh message might cycle in the network. To control the propagation scope of state-refresh messages, you must configure an appropriate hop limit value based on the network size.

Perform the following configurations on all routers in the IPv6 PIM domain.

To configure state-refresh parameters:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure the interval between state-refresh messages.	state-refresh-interval <i>interval</i>	Optional. 60 seconds by default.
4. Configure the time to wait before receiving a new state-refresh message.	state-refresh-rate-limit <i>interval</i>	Optional. 30 seconds by default.
5. Configure the hop limit value of state-refresh messages.	state-refresh-hoplimit <i>hoplimit-value</i>	Optional. 255 by default.

Configuring IPv6 PIM-DM graft retry period

In IPv6 PIM-DM, graft is the only type of message that uses the acknowledgment mechanism. In an IPv6 PIM-DM domain, if a router does not receive a graft-ack message from the upstream router within the specified time after it sends a graft message, the router keeps sending new graft messages at a configurable interval (namely, graft retry period) until it receives a graft-ack message from the upstream router.

To configure the IPv6 PIM-DM graft retry period:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the graft retry period.	pim ipv6 timer graft-retry <i>interval</i>	Optional. 3 seconds by default.

For more information about the configuration of other timers in IPv6 PIM-DM, see "[Configuring IPv6 PIM common timers](#)."

Configuring IPv6 PIM-SM

IPv6 PIM-SM configuration task list

Task	Remarks	
Enabling IPv6 PIM-SM	Required.	
Configuring an RP	Configuring a static RP	Required.
	Configuring a C-RP	Use any approach.
	Enabling embedded RP	
	Configuring C-RP timers globally	Optional.
Configuring a BSR	Configuring a C-BSR	Required.
	Configuring an IPv6 PIM domain border	Optional.
	Configuring C-BSR parameters globally	Optional.
	Configuring C-BSR timers	Optional.
	Disabling BSM semantic fragmentation	Optional.
Configuring IPv6 administrative scoping	Enabling IPv6 administrative scoping	Optional.
	Configuring an IPv6 admin-scope zone boundary	Optional.
	Configuring C-BSRs for IPv6 admin-scope zones	Optional.
Configuring IPv6 multicast source registration	Optional.	

Task	Remarks
Disabling the switchover to SPT	Optional.
Configuring IPv6 PIM common features	Optional.

Configuration prerequisites

Before you configure IPv6 PIM-SM, complete the following tasks:

- Enable IPv6 forwarding and configure an IPv6 unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Determine the IP address of a static RP and the ACL rule defining the range of IPv6 multicast groups to which the static RP is designated.
- Determine the C-RP priority and the ACL rule defining the range of IPv6 multicast groups to which each C-RP is designated.
- Determine the legal C-RP address range and the ACL rule defining the range of IPv6 multicast groups to which the C-RP is designated.
- Determine the C-RP-Adv interval.
- Determine the C-RP timeout.
- Determine the C-BSR priority.
- Determine the hash mask length.
- Determine the IPv6 ACL rule defining a legal BSR address range.
- Determine the BS period.
- Determine the BS timeout.
- Determine the IPv6 ACL rule for register message filtering.
- Determine the register suppression time.
- Determine the register probe time.
- Determine the IPv6 ACL rule and sequencing rule for disabling an SPT switchover.

Enabling IPv6 PIM-SM

With IPv6 PIM-SM enabled, a router sends hello messages periodically to discover IPv6 PIM neighbors and processes messages from the IPv6 PIM neighbors. When you deploy an IPv6 PIM-SM domain, enable IPv6 PIM-SM on all non-border interfaces of the routers.

ⓘ IMPORTANT:

All the interfaces of the same device must operate in the same IPv6 PIM mode.

To enable IPv6 PIM-SM:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IPv6 multicast routing.	multicast ipv6 routing-enable	Disabled by default.
3. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable IPv6 PIM-SM.	pim ipv6 sm	Disabled by default.

Configuring an RP

An RP can be manually configured or dynamically elected through the BSR mechanism. For a large IPv6 PIM network, static RP configuration is a tedious job. Generally, static RP configuration is just a backup method for the dynamic RP election mechanism to enhance the robustness and operation manageability of a multicast network.

! IMPORTANT:

In an IPv6 PIM network, if both IPv6 PIM-SM and IPv6 BIDIR-PIM are enabled, do not configure the same RP to provide services for IPv6 PIM-SM and IPv6 BIDIR-PIM simultaneously to avoid IPv6 PIM routing table errors.

Configuring a static RP

If only one dynamic RP exists in a network, manually configuring a static RP can avoid communication interruption because of single-point failures. It can also avoid frequent message exchange between C-RPs and the BSR.

To enable a static RP to work normally, you must perform this configuration on all routers in the IPv6 PIM-SM domain and specify the same RP address.

Perform the following configuration on all the routers in the IPv6 PIM-SM domain.

To configure a static RP:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure a static RP for IPv6 PIM-SM.	static-rp <i>ipv6-rp-address</i> [<i>acl6-number</i>] [preferred]	No static RP by default.

Configuring a C-RP

In an IPv6 PIM-SM domain, you can configure routers that intend to become the RP as C-RPs. The BSR collects the C-RP information by receiving the C-RP-Adv messages from C-RPs or auto-RP announcements from other routers and organizes the information into an RP-set, which is flooded throughout the entire network. Then, the other routers in the network calculate the mappings between specific group ranges and the corresponding RPs based on the RP-set. HP recommends that you configure C-RPs on backbone routers.

To guard against C-RP spoofing, you need to configure a legal C-RP address range and the range of IPv6 multicast groups to which the C-RP is designated on the BSR. In addition, because every C-BSR has a chance to become the BSR, you need to configure the same filtering policy on all C-BSRs in the IPv6 PIM-SM domain.

When you configure a C-RP, ensure a relatively large bandwidth between this C-RP and the other devices in the IPv6 PIM-SM domain.

To configure a C-RP:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure an interface to be a C-RP for IPv6 PIM-SM.	c-rp ipv6-address [{ group-policy <i>acl6-number</i> scope <i>scope-id</i> } priority <i>priority</i> holdtime <i>hold-interval</i> advertisement-interval <i>adv-interval</i>] *	No C-RPs are configured by default.
4. Configure a legal C-RP address range and the range of IPv6 multicast groups to which the C-RP is designated.	crp-policy <i>acl6-number</i>	Optional. No restrictions by default.

Enabling embedded RP

With the embedded RP feature enabled, the router can resolve the RP address directly from the IPv6 multicast group address of an IPv6 multicast packets. This RP can replace the statically configured RP or the RP dynamically calculated based on the BSR mechanism. Therefore, the DR does not need to identify the RP address beforehand.

Perform this configuration on all routers in the IPv6 PIM-SM domain.

To enable embedded RP:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Enable embedded RP.	embedded-rp [<i>acl6-number</i>]	Optional. By default, embedded RP is enabled for IPv6 multicast groups in the default embedded RP address scopes. The default embedded RP address scopes are FF7x::/12 and FFFx::/12. Here "x" refers to any legal address scope. For more information about the Scope field, see " Multicast overview ."

Configuring C-RP timers globally

To enable the BSR to distribute the RP-set information within the IPv6 PIM-SM domain, C-RPs must periodically send C-RP-Adv messages to the BSR. The BSR obtains the RP-set information from the received messages, and encapsulates its own IPv6 address together with the RP-set information in its bootstrap messages. The BSR then floods the bootstrap messages to all IPv6 routers in the network.

Each C-RP encapsulates a timeout value in its C-RP-Adv messages. After receiving a C-RP-Adv message, the BSR obtains this timeout value and starts a C-RP timeout timer. If the BSR fails to obtain a subsequent C-RP-Adv message from the C-RP when the timer times out, the BSR assumes the C-RP to have expired or become unreachable.

You must configure the C-RP timers on C-RP routers.

To configure C-RP timers globally:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure the C-RP-Adv interval.	c-rp advertisement-interval <i>interval</i>	Optional. 60 seconds by default.
4. Configure C-RP timeout time.	c-rp holdtime <i>interval</i>	Optional. 150 seconds by default.

For more information about the configuration of other timers in IPv6 PIM-SM, see "[Configuring IPv6 PIM common timers](#)."

Configuring a BSR

An IPv6 PIM-SM domain can have only one BSR, but must have at least one C-BSR. Any router can be configured as a C-BSR. Elected from C-BSRs, the BSR is responsible for collecting and advertising RP information in the IPv6 PIM-SM domain.

Configuring a C-BSR

You should configure C-BSRs on routers in the backbone network. When you configure a router as a C-BSR, be sure to specify the IPv6 address of an IPv6 PIM-SM-enabled interface on the router. The BSR election process is as follows:

- Initially, every C-BSR assumes itself to be the BSR of this IPv6 PIM-SM domain and uses its interface IPv6 address as the BSR address to send bootstrap messages.
 - When a C-BSR receives the bootstrap message of another C-BSR, it first compares its own priority with the other C-BSR's priority carried in the message. The C-BSR with a higher priority wins. If a tie exists in the priority, the C-BSR with a higher IPv6 address wins. The loser uses the winner's BSR address to replace its own BSR address and no longer assumes itself to be the BSR, and the winner keeps its own BSR address and continues assuming itself to be the BSR.
- BSR legal address against BSR spoofing

Configuring a legal range of BSR addresses enables filtering of bootstrap messages based on the address range, thereby preventing a maliciously configured host from masquerading as a BSR. You must make the same configuration on all routers in the IPv6 PIM-SM domain. Typical BSR spoofing cases and the corresponding preventive measures are as follows:

- Some maliciously configured hosts can forge bootstrap messages to fool routers and change RP mappings. Such attacks often occur on border routers. Because a BSR is inside the network whereas hosts are outside the network, you can protect a BSR against attacks from external hosts by enabling the border routers to perform neighbor checks and RPF checks on bootstrap messages and to discard unwanted messages.
- If an attacker controls a router in the network or if the network contains an illegal router, the attacker can configure this router as a C-BSR and make it win BSR election to control the right of advertising RP information in the network. After you configure a router as a C-BSR, the router automatically floods the network with bootstrap messages. Because a bootstrap message has a hop limit value of 1, the whole network will not be affected as long as the neighbor router discards these bootstrap messages. Therefore, with a legal BSR address range configured on all routers in the entire network, all these routers will discard bootstrap messages from out of the legal address range.

These preventive measures can partially protect the security of BSRs in a network. However, if an attacker controls a legal BSR, the problem will still occur.

! **IMPORTANT:**

Because a large amount of information needs to be exchanged between a BSR and the other devices in the IPv6 PIM-SM domain, a relatively large bandwidth should be provided between the C-BSR and the other devices in the IPv6 PIM-SM domain.

To configure a C-BSR:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure an interface as a C-BSR.	c-bsr <i>ipv6-address</i> [<i>hash-length</i> [<i>priority</i>]]	No C-BSRs are configured by default.
4. Configure a legal BSR address range.	bsr-policy <i>acl6-number</i>	Optional. No restrictions by default.

Configuring an IPv6 PIM domain border

As the administrative core of an IPv6 PIM-SM domain, the BSR sends the collected RP-set information in the form of bootstrap messages to all routers in the IPv6 PIM-SM domain.

An IPv6 PIM domain border is a bootstrap message boundary. Each BSR has its specific service scope. IPv6 PIM domain border interfaces partition a network into different IPv6 PIM-SM domains. Bootstrap messages cannot cross a domain border in either direction.

Perform the following configuration on routers that you want to configure as an IPv6 PIM domain border.

To configure an IPv6 PIM border domain:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure an IPv6 PIM domain border.	pim ipv6 bsr-boundary	No IPv6 PIM domain border is configured by default.

Configuring C-BSR parameters globally

In each IPv6 PIM-SM domain, a unique BSR is elected from C-BSRs. The C-RPs in the IPv6 PIM-SM domain send advertisement messages to the BSR. The BSR summarizes the advertisement messages to form an RP-set and advertises it to all routers in the IPv6 PIM-SM domain. All the routers use the same hash algorithm to get the RP address that corresponds to specific IPv6 multicast groups.

Perform the following configuration on C-BSR routers.

To configure C-BSR parameters globally:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure the hash mask length.	c-bsr hash-length <i>hash-length</i>	Optional. 126 by default.
4. Configure the C-BSR priority.	c-bsr priority <i>priority</i>	Optional. 64 by default.

Configuring C-BSR timers

The BSR election winner multicasts its own IPv6 address and RP-Set information throughout the region to which it is designated through bootstrap messages. The BSR floods bootstrap messages throughout the network at the interval of the BS (BSR state) period. Any C-BSR that receives a bootstrap message retains the RP-set for the length of BS timeout, during which no BSR election occurs. If no bootstrap message is received from the BSR before the BS timeout timer expires, a new BSR election process begins among the C-BSRs.

Perform the following configuration on C-BSR routers.

To configure C-BSR timers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A

Step	Command	Remarks
3. Configure the BS period.	c-bsr interval <i>interval</i>	Optional. By default, the BS period is determined by the formula "BS period = (BS timeout – 10) / 2." The default BS timeout is 130 seconds, so the default BS period = (130 – 10) / 2 = 60 (seconds). The BS period value must be smaller than the BS timeout value
4. Configure the BS timeout timer.	c-bsr holdtime <i>interval</i>	Optional. By default, the BS timeout value is determined by the formula "BS timeout timer = BS period × 2 + 10." The default BS period is 60 seconds, so the default BS timeout timer = 60 × 2 + 10 = 130 (seconds).

NOTE:

If you configure the BS period or the BS timeout timer, the system uses the configured one instead of the default one.

Disabling BSM semantic fragmentation

Generally, a BSR periodically distributes the RP-set information in bootstrap messages within the IPv6 PIM-SM domain. It encapsulates a BSM in an IPv6 datagram and might split the datagram into fragments if the message exceeds the maximum transmission unit (MTU). In respect of such IP fragmentation, loss of a single IP fragment leads to unavailability of the entire message.

Semantic fragmentation of BSMs can solve this issue. When a BSM exceeds the MTU, it is split to multiple bootstrap message fragments (BSMFs).

- After receiving a BSMF that contains the RP-set information of one group range, a non-BSR router updates corresponding RP-set information directly.
- If the RP-set information of one group range is carried in multiple BSMFs, a non-BSR router updates corresponding RP-set information after receiving all these BSMFs.

Because the RP-set information contained in each segment is different, loss of some IP fragments will not result in dropping of the entire message.

Generally, a BSR performs BSM semantic fragmentation according to the MTU of its BSR interface. However, the semantic fragmentation of BSMs originated because of learning of a new IPv6 PIM neighbor is performed according to the MTU of the outgoing interface.

The function of BSM semantic fragmentation is enabled by default. Devices not supporting this function might deem a fragment as an entire message and learn only part of the RP-set information. Therefore, if such devices exist in the IPv6 PIM-SM domain, you need to disable the semantic fragmentation function on the C-BSRs.

To disable the BSM semantic fragmentation function:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Disable the BSM semantic fragmentation function.	undo bsm-fragment enable	By default, the BSM semantic fragmentation function is enabled.

Configuring IPv6 administrative scoping

With IPv6 administrative scoping disabled, an IPv6 PIM-SM domain has only one BSR. The BSR manages the whole network. To manage your network more effectively and specifically, you can partition the IPv6 PIM-SM domain into multiple IPv6 admin-scope zones. Each IPv6 admin-scope zone maintains a BSR, which provides services for a specific IPv6 multicast group range. The IPv6 global scope zone also maintains a BSR, which provides services for the IPv6 multicast groups with the Scope field in the group addresses being 14.

Enabling IPv6 administrative scoping

Before you configure an IPv6 admin-scope zone, you must enable IPv6 administrative scoping.

Perform the following configuration on all routers in the IPv6 PIM-SM domain.

To enable IPv6 administrative scoping:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Enable IPv6 administrative scoping.	c-bsr admin-scope	Disabled by default

Configuring an IPv6 admin-scope zone boundary

The boundary of each IPv6 admin-scope zone is formed by ZBRs. Each admin-scope zone maintains a BSR, which provides services for multicast groups with a specific Scope field in their group addresses. Multicast protocol packets (such as assert messages and bootstrap messages) that belong to this range cannot cross the admin-scope zone boundary.

Perform the following configuration on routers that you want to configure as a ZBR.

To configure an IPv6 admin-scope zone boundary:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type interface-number</i>	N/A

Step	Command	Remarks
3. Configure an IPv6 multicast forwarding boundary.	multicast ipv6 boundary { <i>ipv6-group-address prefix-length</i> scope { <i>scope-id</i> admin-local global organization-local site-local } }	By default, no multicast forwarding boundary is configured.

Configuring C-BSRs for IPv6 admin-scope zones

In a network with IPv6 administrative scoping enabled, BSRs are elected from C-BSRs specific to different Scope field values. The C-RPs in the network send advertisement messages to the specific BSR. The BSR summarizes the advertisement messages to form an RP-set and advertises it to all routers in the specific admin-scope zone. All the routers use the same hash algorithm to get the RP address corresponding to the specific IPv6 multicast group.

You can configure the hash mask length and C-BSR priority globally and in an IPv6 admin-scope zone.

- The values configured in the IPv6 admin-scope zone have preference over the global values.
- If you do not configure these parameters in the IPv6 admin-scope zone, the corresponding global values will be used.

For configuration of global C-BSR parameters, see "[Configuring C-BSR parameters globally.](#)"

Perform the following configuration on the routers that you want to configure as C-BSRs in IPv6 admin-scope zones.

To configure a C-BSR for an IPv6 admin-scope zone:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure a C-BSR for an IPv6 admin-scope zone.	c-bsr scope { <i>scope-id</i> admin-local global organization-local site-local } [hash-length <i>hash-length</i> priority <i>priority</i>] *	No C-BSRs are configured for an IPv6 admin-scope zone by default.

Configuring IPv6 multicast source registration

Within an IPv6 PIM-SM domain, the source-side DR sends register messages to the RP, and these register messages have different IPv6 multicast source or IPv6 multicast group addresses. You can configure a filtering rule to filter register messages so that the RP can provide services for specific IPv6 multicast groups. If the filtering rule denies an (S, G) entry, or if the filtering rule does not define an action for this entry, the RP will send a register-stop message to the DR to stop the registration process for the IPv6 multicast data.

In view of information integrity of register messages in the transmission process, you can configure the device to calculate the checksum based on the entire register messages. However, to reduce the workload of encapsulating data in register messages and for the sake of interoperability, HP does not recommend this method of checksum calculation.

When receivers stop receiving data addressed to a certain IPv6 multicast group through the RP (which means that the RP stops serving the receivers of that IPv6 multicast group), or when the RP starts receiving IPv6 multicast data from the IPv6 multicast source along the SPT, the RP sends a register-stop message to the source-side DR. After receiving this message, the DR stops sending register messages encapsulated with IPv6 multicast data and starts a register-stop timer. Before the register-stop timer expires, the DR sends a null register message (a register message without multicast data) to the RP. If the DR receives a register-stop message during the register probe time, it will reset its register-stop timer. Otherwise, the DR starts sending register messages with encapsulated data again when the register-stop timer expires.

The register-stop timer is set to a random value chosen uniformly from the interval (0.5 times register_suppression_time, 1.5 times register_suppression_time) minus register_probe_time.

Configure a filtering rule for register messages on all C-RP routers, and configure them to calculate the checksum based on the entire register messages. Configure the register suppression time and the register probe time on all routers that might become IPv6 source-side DRs.

To configure register-related parameters:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure a filtering rule for register messages.	register-policy <i>acl6-number</i>	Optional. No register filtering rule by default.
4. Configure the device to calculate the checksum based on the entire register messages.	register-whole-checksum	Optional. Based on the header of register messages by default.
5. Configure the register suppression time.	register-suppression-timeout <i>interval</i>	Optional. 60 seconds by default.
6. Configure the register probe time.	probe-interval <i>interval</i>	Optional. 5 seconds by default.

Disabling the switchover to SPT

⚠ CAUTION:

If the switch is an RP, disabling switchover to SPT might cause multicast traffic forwarding failures on the source-side DR. When disabling switchover to SPT, be sure you fully understand its impact on your network.

If the switch acts as an RP or the receiver-side DR, it initiates the switchover to SPT by default upon receiving the first IPv6 multicast packet along the RPT. You can disable the switchover from RPT to SPT.

To configure the switchover to SPT:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Disable the switchover to SPT.	spt-switch-threshold infinity [group-policy <i>acl6-number</i> [order <i>order-value</i>]]	Optional. By default, the device switches to the SPT immediately after it receives the first IPv6 multicast packet from the RPT.

Configuring IPv6 BIDIR-PIM

IPv6 BIDIR-PIM configuration task list

Task	Remarks	
Enabling IPv6 PIM-SM	Required.	
Enabling IPv6 BIDIR-PIM	Required.	
Configuring an RP	Configuring a static RP	Required.
	Configuring a C-RP	Use any approach.
	Enabling embedded RP	
	Configuring C-RP timers globally	Optional.
Configuring a BSR	Configuring a C-BSR	Required.
	Configuring an IPv6 BIDIR-PIM domain border	Optional.
	Configuring global C-BSR parameters	Optional.
	Configuring C-BSR timers	Optional.
	Disabling BSM semantic fragmentation	Optional.
Configuring IPv6 administrative scoping	Enabling IPv6 administrative scoping	Optional.
	Configuring an IPv6 admin-scope zone boundary	Optional.
	Configuring C-BSRs for each admin-scope zone	Optional.
Configuring IPv6 PIM common features	Optional.	

Configuration prerequisites

Before you configure IPv6 BIDIR-PIM, complete the following tasks:

- Enable IPv6 forwarding and configure an IPv6 unicast routing protocol so that all devices in the domain can communicate with each other at Layer 3.
- Determine the IPv6 address of a static RP and the IPv6 ACL that defines the range of IPv6 multicast groups to which the static RP is designated.

- Determine the C-RP priority and the IPv6 ACL that defines the range of IPv6 multicast groups to which each C-RP is designated.
- Determine the legal C-RP address range and the IPv6 ACL that defines the range of IPv6 multicast groups to which the C-RP is designated.
- Determine the C-RP-Adv interval.
- Determine the C-RP timeout.
- Determine the C-BSR priority.
- Determine the hash mask length.
- Determine the IPv6 ACL defining the legal BSR address range.
- Determine the BS period.
- Determine the BS timeout.

Enabling IPv6 PIM-SM

You must enable IPv6 PIM-SM before enabling IPv6 BIDIR-PIM because IPv6 BIDIR-PIM is implemented on the basis of IPv6 PIM-SM. To deploy an IPv6 BIDIR-PIM domain, enable IPv6 PIM-SM on all non-border interfaces of the domain.

! IMPORTANT:

On a router, all interfaces in the same VPN instance must operate in the same IPv6 PIM mode.

To enable IPv6 PIM-SM:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IPv6 multicast routing.	multicast ipv6 routing-enable	Disabled by default
3. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable IPv6 PIM-SM.	pim ipv6 sm	Disabled by default

Enabling IPv6 BIDIR-PIM

Perform this configuration on all routers in the IPv6 BIDIR-PIM domain.

To enable IPv6 BIDIR-PIM:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Enable IPv6 BIDIR-PIM.	bidir-pim enable	Disabled by default

Configuring an RP

An RP can be manually configured or dynamically elected through the BSR mechanism. For a large IPv6 PIM network, static RP configuration is a tedious job. Generally, static RP configuration is just a backup means for the dynamic RP election mechanism to enhance the robustness and operation manageability of a multicast network.

! IMPORTANT:

In an IPv6 PIM network, if both IPv6 PIM-SM and IPv6 BIDIR-PIM are enabled, do not configure the same RP to provide services for IPv6 PIM-SM and IPv6 BIDIR-PIM simultaneously to avoid IPv6 PIM routing table errors.

Configuring a static RP

If only one dynamic RP exists in a network, manually configuring a static RP can avoid communication interruption because of single-point failures and avoid frequent message exchange between C-RPs and the BSR.

In IPv6 BIDIR-PIM, a static RP can be specified with a virtual IPv6 address. For example, if the IPv6 addresses of the interfaces at the two ends of a link are 1001::1/64 and 1001::2/64, you can specify a virtual IPv6 address, like 1001::100/64, for the static RP. As a result, the link becomes an RPL.

To make a static RP to work normally, you must perform this configuration on all routers in the IPv6 BIDIR-PIM domain and specify the same RP address.

To configure a static RP:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure a static RP for IPv6 BIDIR-PIM.	static-rp <i>ipv6-rp-address</i> [<i>acl6-number</i>] [preferred] bidir	No static RP by default

Configuring a C-RP

In an IPv6 BIDIR-PIM domain, you can configure routers that intend to become the RP as C-RPs. The BSR collects the C-RP information by receiving the C-RP-Adv messages from C-RPs or auto-RP announcements from other routers and organizes the information into an RP-set, which is flooded throughout the entire network. Then, the other routers in the network calculate the mappings between specific group ranges and the corresponding RPs based on the RP-set. HP recommends that you configure C-RPs on backbone routers.

To guard against C-RP spoofing, configure a legal C-RP address range and the range of multicast groups to which the C-RP is designated on the BSR. In addition, because every C-BSR has a chance to become the BSR, you must configure the same filtering policy on all C-BSRs in the IPv6 BIDIR-PIM domain.

When you configure a C-RP, ensure a relatively large bandwidth between this C-RP and the other devices in the IPv6 BIDIR-PIM domain.

To configure a C-RP:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure an interface to be a C-RP for IPv6 BIDIR-PIM.	c-rp ipv6-address [{ group-policy <i>acl6-number</i> scope <i>scope-id</i> } priority <i>priority</i> holdtime <i>hold-interval</i> advertisement-interval <i>adv-interval</i>] * bidir	No C-RP is configured by default.

Enabling embedded RP

With the embedded RP feature enabled, the router can resolve the RP address directly from the IPv6 multicast group address of an IPv6 multicast packets. This RP can replace the statically configured RP or the RP dynamically calculated based on the BSR mechanism. Thus, the DR does not need to know the RP address beforehand.

Perform this configuration on all routers in the IPv6 BIDIR-PIM domain.

To enable embedded RP:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Enable embedded RP.	embedded-rp [<i>acl6-number</i>]	Optional. By default, embedded RP is enabled for IPv6 multicast groups in the default embedded RP address scopes. The default embedded RP address scopes are FF7x::/12 and FFFx::/12, where x refers to any legal address scope. For more information about the Scope field, see " Multicast overview ."

Configuring C-RP timers globally

To enable the BSR to distribute the RP-Set information within the IPv6 BIDIR-PIM domain, C-RPs must periodically send C-RP-Adv messages to the BSR. The BSR learns the RP-Set information from the received messages, and encapsulates its own IPv6 address together with the RP-Set information in its bootstrap messages. The BSR then floods the bootstrap messages to all IPv6 routers in the network.

Each C-RP encapsulates a timeout value in its C-RP-Adv messages. After receiving a C-RP-Adv message, the BSR obtains this timeout value and starts a C-RP timeout timer. If the BSR fails to hear a subsequent C-RP-Adv message from the C-RP when the timer times out, the BSR assumes the C-RP to have expired or become unreachable.

The C-RP timers need to be configured on C-RP routers.

To configure C-RP timers globally:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure the C-RP-Adv interval.	c-rp advertisement-interval <i>interval</i>	Optional. 60 seconds by default.
4. Configure C-RP timeout time.	c-rp holdtime <i>interval</i>	Optional. 150 seconds by default.

For more information about the configuration of other timers in IPv6 PIM-SM, see "[Configuring IPv6 PIM common timers](#)."

Configuring a BSR

An IPv6 BIDIR-PIM domain can have only one BSR, but must have at least one C-BSR. Any router can be configured as a C-BSR. Elected from C-BSRs, the BSR collects and advertises RP information in the IPv6 BIDIR-PIM domain.

Configuring a C-BSR

C-BSRs must be configured on routers on the backbone network. When you configure a router as a C-BSR, be sure to specify an IPv6 PIM-SM-enabled interface on the router. The BSR election process is as follows:

- Initially, every C-BSR assumes itself to be the BSR of the IPv6 BIDIR-PIM domain, and uses its interface IPv6 address as the BSR address to send bootstrap messages.
- When a C-BSR receives the bootstrap message of another C-BSR, it first compares its own priority with the other C-BSR's priority carried in message. The C-BSR with a higher priority wins. If a tie exists in the priority, the C-BSR with a higher IPv6 address wins. The loser uses the winner's BSR address to replace its own BSR address and no longer assumes itself to be the BSR, and the winner retains its own BSR address and continues assuming itself to be the BSR.

Configuring a legal range of BSR addresses enables filtering of bootstrap messages based on the address range, thus to prevent a maliciously configured host from masquerading as a BSR. The same configuration must be made on all routers in the IPv6 BIDIR-PIM domain. The following are typical BSR spoofing cases and the corresponding preventive measures:

- Some maliciously configured hosts can forge bootstrap messages to fool routers and change RP mappings. Such attacks often occur on border routers. Because a BSR is inside the network whereas hosts are outside the network, you can protect a BSR against attacks from external hosts by enabling the border routers to perform neighbor checks and RPF checks on bootstrap messages and discard unwanted messages.
- When a router in the network is controlled by an attacker or when an illegal router is present in the network, the attacker can configure this router as a C-BSR and make it win BSR election to control

the right of advertising RP information in the network. After being configured as a C-BSR, a router automatically floods the network with bootstrap messages. Because a bootstrap message has a hop limit value of 1, the whole network will not be affected as long as the neighbor router discards these bootstrap messages. Therefore, with a legal BSR address range configured on all routers in the entire network, all these routers will discard bootstrap messages from out of the legal address range.

The preventive measures can partially protect the security of BSRs in a network. However, if a legal BSR is controlled by an attacker, the preceding problem will still occur.

! **IMPORTANT:**

Because a large amount of information will be exchanged between a BSR and the other devices in the IPv6 BIDIR-PIM domain, a relatively large bandwidth should be provided between the C-BSRs and the other devices in the IPv6 BIDIR-PIM domain.

To configure a C-BSR:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure an interface as a C-BSR.	c-bsr <i>ipv6-address</i> [<i>hash-length</i> [<i>priority</i>]]	No C-BSRs are configured by default.
4. Configure a legal BSR address range.	bsr-policy <i>acl6-number</i>	Optional. No restrictions on BSR address range by default.

Configuring an IPv6 BIDIR-PIM domain border

As the administrative core of an IPv6 BIDIR-PIM domain, the BSR sends the collected RP-Set information in the form of bootstrap messages to all routers in the IPv6 BIDIR-PIM domain.

An IPv6 BIDIR-PIM domain border is a bootstrap message boundary. Each BSR has its specific service scope. A number of IPv6 BIDIR-PIM domain border interfaces partition a network into different IPv6 BIDIR-PIM domains. Bootstrap messages cannot cross a domain border in either direction.

Perform the following configuration on routers that you want to configure as the IPv6 BIDIR-PIM domain border.

To configure an IPv6 BIDIR-PIM domain border:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure an IPv6 BIDIR-PIM domain border.	pim ipv6 bsr-boundary	By default, no IPv6 BIDIR-PIM domain border is configured.

Configuring global C-BSR parameters

In each IPv6 BIDIR-PIM domain, a unique BSR is elected from C-BSRs. The C-RPs in the IPv6 BIDIR-PIM domain send advertisement messages to the BSR. The BSR summarizes the advertisement messages to form an RP-set and advertises it to all routers in the IPv6 BIDIR-PIM domain. All the routers use the same hash algorithm to get the RP address corresponding to specific multicast groups.

Perform the following configuration on C-BSR routers.

To configure global C-BSR parameters:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure the hash mask length.	c-bsr hash-length <i>hash-length</i>	Optional. 126 by default.
4. Configure the C-BSR priority.	c-bsr priority <i>priority</i>	Optional. 64 by default.

Configuring C-BSR timers

The BSR election winner multicasts its own IPv6 address and RP-Set information through bootstrap messages within the entire zone to which it is designated. The BSR floods bootstrap messages throughout the network at the interval of BS (BSR state) period. Any C-BSR that receives a bootstrap message retains the RP-set for the length of BS timeout, during which no BSR election takes place. If no bootstrap message is received from the BSR before the BS timeout timer expires, a new BSR election process is triggered among the C-BSRs.

Perform the following configuration on C-BSR routers.

To configure C-BSR timers:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure the BS period.	c-bsr interval <i>interval</i>	Optional. By default, the BS period is determined by the formula "BS period = (BS timeout – 10) / 2." The default BS timeout is 130 seconds, so the default BS period = (130 – 10) / 2 = 60 (seconds). The BS period value must be smaller than the BS timeout value.

Step	Command	Remarks
4.	Configure the BS timeout timer.	Optional. By default, the BS timeout value is determined by the formula "BS timeout timer = BS period × 2 + 10." The default BS period is 60 seconds, so the default BS timeout timer = 60 × 2 + 10 = 130 (seconds).

NOTE:

If you configure the BS period or the BS timeout timer, the system uses the configured one instead of the default one.

Disabling BSM semantic fragmentation

Generally, a BSR periodically distributes the RP-set information in bootstrap messages within the IPv6 BIDIR-PIM domain. It encapsulates a BSM in an IP datagram and might split the datagram into fragments if the message exceeds the maximum transmission unit (MTU). In respect of such IP fragmentation, loss of a single IP fragment leads to unavailability of the entire message.

Semantic fragmentation of BSMs can solve this issue. When a BSM exceeds the MTU, it is split to multiple bootstrap message fragments (BSMFs).

- After receiving a BSMF that contains the RP-set information of one group range, a non-BSR router updates corresponding RP-set information directly.
- If the RP-set information of one group range is carried in multiple BSMFs, a non-BSR router updates corresponding RP-set information after receiving all these BSMFs.

Because the RP-set information contained in each segment is different, loss of some IP fragments will not result in dropping of the entire message.

Generally, a BSR performs BSM semantic fragmentation according to the MTU of its BSR interface. However, the semantic fragmentation of BSMs originated because of learning of a new PIM neighbor is performed according to the MTU of the outgoing interface.

The function of BSM semantic fragmentation is enabled by default. Devices not supporting this function might deem a fragment as an entire message, thus learning only part of the RP-set information. Therefore, if such devices exist in the IPv6 BIDIR-PIM domain, you need to disable the semantic fragmentation function on the C-BSRs.

To disable the BSM semantic fragmentation function:

Step	Command	Remarks
1.	Enter system view.	N/A
2.	Enter IPv6 PIM view.	N/A
3.	Disable the BSM semantic fragmentation function.	By default, the BSM semantic fragmentation function is enabled.

Configuring IPv6 administrative scoping

With administrative scoping disabled, an IPv6 BIDIR-PIM domain has only one BSR. The BSR manages the whole network. To manage your network more effectively and specifically, you can partition the IPv6 BIDIR-PIM domain into multiple admin-scope zones. Each admin-scope zone maintains a BSR, which provides services for a specific multicast group range. The global scope zone also maintains a BSR, which provides services for all the rest multicast groups.

Enabling IPv6 administrative scoping

Before you configure an IPv6 admin-scope zone, you must enable IPv6 administrative scoping first.

Perform the following configuration on all routers in the IPv6 PIM-SM domain.

To enable IPv6 administrative scoping:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Enable IPv6 administrative scoping.	c-bsr admin-scope	Disabled by default

Configuring an IPv6 admin-scope zone boundary

The boundary of each IPv6 admin-scope zone is formed by ZBRs. Each admin-scope zone maintains a BSR, which provides services for a specific IPv6 multicast group range. IPv6 multicast packets (such as assert messages and bootstrap messages) that belong to this range cannot cross the admin-scope zone boundary.

Perform the following configuration on routers that you want to configure as a ZBR.

To configure an admin-scope zone boundary:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure an IPv6 multicast forwarding boundary.	multicast ipv6 boundary { <i>ipv6-group-address prefix-length</i> scope { <i>scope-id</i> admin-local global organization-local site-local } }	By default, no IPv6 multicast forwarding boundary is configured.

For more information about the **multicast ipv6 boundary** command, see *IP Multicast Command Reference*.

Configuring C-BSRs for each admin-scope zone

In a network with administrative scoping enabled, group-range-specific BSRs are elected from C-BSRs. C-RPs in the network send advertisement messages to the specific BSR. The BSR summarizes the

advertisement messages to form an RP-set and advertises it to all routers in the specific admin-scope zone. All the routers use the same hash algorithm to get the RP address corresponding to the specific multicast group.

You can configure the hash mask length and C-BSR priority globally, only in an IPv6 admin-scope zone, or both globally and in an IPv6 admin-scope zone.

- The values configured in the IPv6 admin-scope zone have preference over the global values.
- If you do not configure these parameters in the IPv6 admin-scope zone, the corresponding global values will be used.

For configuration of global C-BSR parameters, see "[Configuring global C-BSR parameters.](#)"

Perform the following configuration on the routers that you want to configure as C-BSRs in admin-scope zones.

To configure a C-BSR for an admin-scope zone:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure a C-BSR for an admin-scope zone.	c-bsr scope { <i>scope-id</i> admin-local global organization-local site-local } [hash-length <i>hash-length</i> priority <i>priority</i>] *	No C-BSRs are configured for an admin-scope zone by default.

Configuring IPv6 PIM-SSM

The IPv6 PIM-SSM model needs the support of MLDv2. Be sure to enable MLDv2 on IPv6 PIM routers with receivers attached to them.

IPv6 PIM-SSM configuration task list

Task	Remarks
Enabling IPv6 PIM-SSM	Required
Configuring the IPv6 SSM group range	Optional
Configuring IPv6 PIM common features	Optional

Configuration prerequisites

Before you configure IPv6 PIM-SSM, complete the following tasks:

- Enable IPv6 forwarding and configure an IPv6 unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Determine the IPv6 SSM group range.

Enabling IPv6 PIM-SM

When you enable IPv6 PIM-SM, follow these guidelines:

- The SSM model is implemented based on some subsets of IPv6 PIM-SM. Therefore, you must enable IPv6 PIM-SM before configuring IPv6 PIM-SSM.
- When you deploy an IPv6 PIM-SSM domain, enable IPv6 PIM-SM on all non-border interfaces of routers.
- All the interfaces of the same device must operate in the same IPv6 PIM mode.

To enable IPv6 PIM-SSM:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable IPv6 multicast routing.	multicast ipv6 routing-enable	Disabled by default
3. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Enable IPv6 PIM-SM.	pim ipv6 sm	Disabled by default

Configuring the IPv6 SSM group range

Whether the information from an IPv6 multicast source is delivered to the receivers based on the IPv6 PIM-SSM model or the IPv6 PIM-SM model depends on whether the group address in the (S, G) channel subscribed by the receivers falls into the IPv6 SSM group range. All IPv6 PIM-SM-enabled interfaces assume that IPv6 multicast groups within this address range are using the IPv6 SSM model.

Configuration guidelines

- Make sure the same IPv6 SSM group range is configured on all routers in the entire domain. Otherwise, IPv6 multicast data cannot be delivered through the IPv6 SSM model.
- When a member of an IPv6 multicast group in the IPv6 SSM group range sends an MLDv1 report message, the device does not trigger a (*, G) join.

Configuration procedure

Perform the following configuration on all routers in the IPv6 PIM-SSM domain.

To configure the IPv6 SSM group range:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure the IPv6 SSM group range.	ssm-policy <i>acl6-number</i>	Optional. FF3x::/32 by default, here "x" refers to any legal group scope.

Configuring IPv6 PIM common features

For the configuration tasks in this section:

- In IPv6 PIM view, the configuration is effective on all interfaces. In interface view, the configuration is effective on only the current interface.
- If the same function or parameter is configured in both IPv6 PIM view and interface view, the configuration in interface view has preference over the configuration in PIM view, regardless of the configuration sequence.

IPv6 PIM common feature configuration task list

Task	Remarks
Configuring an IPv6 multicast data filter	Optional
Configuring a hello message filter	Optional
Configuring IPv6 PIM hello options	Optional
Configuring the prune delay	Optional
Configuring IPv6 PIM common timers	Optional
Configuring join/prune message sizes	Optional
Configuring IPv6 PIM to work with BFD	Optional
Setting the DSCP value for IPv6 PIM messages	Optional

Configuration prerequisites

Before you configure IPv6 PIM common features, complete the following tasks:

- Enable IPv6 forwarding and configure an IPv6 unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Configure IPv6 PIM-DM (or IPv6 PIM-SM or IPv6 PIM-SSM).
- Determine the IPv6 ACL rule for filtering IPv6 multicast data.
- Determine the IPv6 ACL rule defining a legal source address range for hello messages.
- Determine the priority for DR election (global value/interface level value).
- Determine the IPv6 PIM neighbor timeout time (global value/interface value).
- Determine the prune message delay (global value/interface level value).
- Determine the prune override interval (global value/interface level value).
- Determine the prune delay.
- Determine the hello interval (global value/interface level value).
- Determine the maximum delay between hello message (interface level value).
- Determine the assert timeout time (global value/interface value).

- Determine the join/prune interval (global value/interface level value).
- Determine the join/prune timeout (global value/interface value).
- Determine the IPv6 multicast source lifetime.
- Determine the maximum size of join/prune messages.
- Determine the maximum number of (S, G) entries in a join/prune message.
- Determine the DSCP value for IPv6 PIM messages.

Configuring an IPv6 multicast data filter

In either an IPv6 PIM-DM domain or an IPv6 PIM-SM domain, routers can check passing-by IPv6 multicast data based on the configured filtering rules and determine whether to continue forwarding the IPv6 multicast data. In other words, IPv6 PIM routers can act as IPv6 multicast data filters. These filters can help implement traffic control on one hand, and control the information available to downstream receivers to enhance data security on the other hand.

Configuration guidelines

- Generally, a smaller distance from the filter to the IPv6 multicast source results in a more remarkable filtering effect.
- This filter works not only on independent IPv6 multicast data but also on IPv6 multicast data encapsulated in register messages.

Configuration procedure

To configure an IPv6 multicast data filter:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure an IPv6 multicast group filter.	source-policy <i>acl6-number</i>	No IPv6 multicast data filter by default

Configuring a hello message filter

Along with the wide applications of IPv6 PIM, the security requirement for the protocol is becoming increasingly demanding. The establishment of correct IPv6 PIM neighboring relationships is a prerequisite for secure application of IPv6 PIM. To guide against IPv6 PIM message attacks, you can configure a legal source address range for hello messages on interfaces of routers to ensure the correct IPv6 PIM neighboring relationships.

To configure a hello message filter:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure a hello message filter.	pim ipv6 neighbor-policy <i>acl6-number</i>	No hello message filter by default

NOTE:

With the hello message filter configured, if hello messages of an existing IPv6 PIM neighbor fail to pass the filter, the IPv6 PIM neighbor will be removed automatically when it times out.

Configuring IPv6 PIM hello options

In either an IPv6 PIM-DM domain or an IPv6 PIM-SM domain, the hello messages sent among routers contain the following configurable options:

- **DR_Priority** (for IPv6 PIM-SM only)—Priority for DR election. The higher the priority is, the easier it is for the router to win DR election. You can configure this parameter on all the routers in a multi-access network directly connected to IPv6 multicast sources or receivers.
- **Holdtime**—The timeout time of IPv6 PIM neighbor reachability state. When this timer times out, if the router has received no hello message from an IPv6 PIM neighbor, it assumes that this neighbor has expired or become unreachable.
- **LAN_Prune_Delay**—The delay of prune messages on a multi-access network. This option consists of LAN-delay (namely, prune message delay), override-interval, and neighbor tracking flag. If the LAN-delay or override-interval values of different IPv6 PIM routers on a multi-access subnet are different, the largest value takes effect. If you want to enable neighbor tracking, be sure to enable the neighbor tracking feature on all IPv6 PIM routers on a multi-access subnet.

The LAN-delay setting will cause the upstream routers to delay forwarding received prune messages. The override-interval sets the length of time that a downstream router can wait before sending a prune override message. When a router receives a prune message from a downstream router, it does not perform the prune action immediately. Instead, it maintains the current forwarding state for a period of LAN-delay plus override-interval. If the downstream router needs to continue receiving IPv6 multicast data, it must send a join message within the prune override interval. Otherwise, the upstream route will perform the prune action when the period of LAN-delay plus override-interval times out.

A hello message sent from an IPv6 PIM router contains a generation ID option. The generation ID is a random value for the interface on which the hello message is sent. Normally, the generation ID of an IPv6 PIM router does not change unless the status of the router changes (for example, when IPv6 PIM is just enabled on the interface or the device is restarted). When the router starts or restarts sending hello messages, it generates a new generation ID. If an IPv6 PIM router finds that the generation ID in a hello message from the upstream router has changed, it assumes that the status of the upstream neighbor is lost or that the upstream neighbor has changed. In this case, it triggers a join message for state update.

If you disable join suppression (namely, enable neighbor tracking), be sure to disable the join suppression feature on all IPv6 PIM routers on a multi-access subnet. Otherwise, the upstream router will fail to explicitly track join messages from downstream routers.

Configuring hello options globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure the priority for DR election.	hello-option dr-priority <i>priority</i>	Optional. 1 by default.
4. Configure IPv6 PIM neighbor timeout time.	hello-option holdtime <i>interval</i>	Optional. 105 seconds by default.
5. Configure the prune message delay time (LAN-delay).	hello-option lan-delay <i>interval</i>	Optional. 500 milliseconds by default.
6. Configure the prune override interval.	hello-option override-interval <i>interval</i>	Optional. 2,500 milliseconds by default.
7. Disable join suppression.	hello-option neighbor-tracking	Enabled by default.

Configuring hello options on an interface

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the priority for DR election.	pim ipv6 hello-option dr-priority <i>priority</i>	Optional. 1 by default.
4. Configure IPv6 PIM neighbor timeout time.	pim ipv6 hello-option holdtime <i>interval</i>	Optional. 105 seconds by default.
5. Configure the prune message delay time (LAN-delay).	pim ipv6 hello-option lan-delay <i>interval</i>	Optional. 500 milliseconds by default.
6. Configure the prune override interval.	pim ipv6 hello-option override-interval <i>interval</i>	Optional. 2500 milliseconds by default.
7. Disable join suppression.	pim ipv6 hello-option neighbor-tracking	Enabled by default.
8. Configure the interface to reject hello messages without a generation ID.	pim ipv6 require-genid	By default, hello messages without Generation_ID are accepted.

Configuring the prune delay

Configuring the prune delay interval on an upstream router in a shared network segment can make the upstream router not perform the prune action immediately after receiving the prune message from its downstream router. Instead, the upstream router maintains the current forwarding state for a period of time that the prune delay interval defines. In this period, if the upstream router receives a join message from the downstream router, it cancels the prune action. Otherwise, it performs the prune action.

To configure the prune delay time

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure the prune delay interval.	prune delay <i>interval</i>	Optional. By default, the prune delay is not configured.

Configuring IPv6 PIM common timers

IPv6 PIM routers discover IPv6 PIM neighbors and maintain IPv6 PIM neighboring relationships with other routers by periodically sending hello messages.

After receiving a hello message, an IPv6 PIM router waits a random period, which is smaller than the maximum delay between hello messages, before sending a hello message. This avoids collisions that occur when multiple IPv6 PIM routers send hello messages simultaneously.

An IPv6 PIM router periodically sends join/prune messages to its upstream for state update. A join/prune message contains the join/prune timeout time. The upstream router sets a join/prune timeout timer for each pruned downstream interface.

Any router that has lost assert election will prune its downstream interface and maintain the assert state for a period of time. When the assert state times out, the assert loser will resume IPv6 multicast forwarding.

When a router fails to receive subsequent IPv6 multicast data from the IPv6 multicast source *S*, the router does not immediately delete the corresponding (*S*, *G*) entry. Instead, it maintains the (*S*, *G*) entry for a period of time—namely, the IPv6 multicast source lifetime—before deleting the (*S*, *G*) entry.

NOTE:

If no special networking requirements are raised, use the default settings.

Configuring IPv6 PIM common timers globally

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure the hello interval.	timer hello <i>interval</i>	Optional. 30 seconds by default.
4. Configure the join/prune interval.	timer join-prune <i>interval</i>	Optional. 60 seconds by default.
5. Configure the join/prune timeout time.	holdtime join-prune <i>interval</i>	Optional. 210 seconds by default.
6. Configure assert timeout time.	holdtime assert <i>interval</i>	Optional. 180 seconds by default.
7. Configure the IPv6 multicast source lifetime.	source-lifetime <i>interval</i>	Optional. 210 seconds by default.

Configuring IPv6 PIM common timers on an interface

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure the hello interval.	pim ipv6 timer hello <i>interval</i>	Optional. 30 seconds by default.
4. Configure the maximum delay between hello messages.	pim ipv6 triggered-hello-delay <i>interval</i>	Optional. 5 seconds by default.
5. Configure the join/prune interval.	pim ipv6 timer join-prune <i>interval</i>	Optional. 60 seconds by default.
6. Configure the join/prune timeout time.	pim ipv6 holdtime join-prune <i>interval</i>	Optional. 210 seconds by default.
7. Configure assert timeout time.	pim ipv6 holdtime assert <i>interval</i>	Optional 180 seconds by default.

Configuring join/prune message sizes

A large size of a join/prune message might result in loss of a larger amount of information if a message is lost. You can set a small value for the size of each join/prune message to reduce the impact in case of the loss of a message.

By controlling the maximum number of (S, G) entries in a join/prune message, you can effectively reduce the number of (S, G) entries sent per unit of time.

! **IMPORTANT:**

If IPv6 PIM snooping-enabled switches are deployed in the IPv6 PIM network, be sure to set a value no greater than the IPv6 path MTU for the maximum size of each join/prune message on the receiver-side edge IPv6 PIM devices.

To configure join/prune message sizes:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Configure the maximum size of each join/prune message.	jp-pkt-size <i>packet-size</i>	Optional. 8100 bytes by default.
4. Configure the maximum number of (S, G) entries in a join/prune message.	jp-queue-size <i>queue-size</i>	Optional. 1020 by default.

Configuring IPv6 PIM to work with BFD

IPv6 PIM uses hello messages to elect a DR for a multi-access network. The elected DR will be the only multicast forwarder on the multi-access network.

If the DR fails, a new DR election process will start after the DR is aged out. However, it might take a long period of time. To start a new DR election process immediately after the original DR fails, you can enable IPv6 PIM to work with Bidirectional Forwarding Detection (BFD) on a multi-access network to detect failures of the links among IPv6 PIM neighbors. You must enable IPv6 PIM to work with BFD on all IPv6 PIM-capable routers on a multi-access network, so that the IPv6 PIM neighbors can fast detect DR failures and start a new DR election process.

Before you configure this feature on an interface, be sure to enable IPv6 PIM-DM or IPv6 PIM-SM on the interface.

To enable IPv6 PIM to work with BFD:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter interface view.	interface <i>interface-type interface-number</i>	N/A
3. Enable IPv6 PIM to work with BFD.	pim ipv6 bfd enable	Disabled by default

For more information about BFD, see *High Availability Configuration Guide*.

Setting the DSCP value for IPv6 PIM messages

IPv6 uses an eight-bit Traffic class field (called ToS in IPv4) to identify type of service for IP packets. As defined in RFC 2474, the first six bits contains the DSCP priority for prioritizing traffic in the network and the last two bits are reserved.

To set the DSCP value for IPv6 PIM messages:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter IPv6 PIM view.	pim ipv6	N/A
3. Set the DSCP value for IPv6 PIM messages.	dscp <i>dscp-value</i>	Optional. By default, the DSCP value in IPv6 PIM messages is 48.

Displaying and maintaining IPv6 PIM

Task	Command	Remarks
Display the BSR information in the IPv6 PIM-SM domain and locally configured C-RP information in effect.	display pim ipv6 bsr-info [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display information about IPv6 unicast routes used by IPv6 PIM.	display pim ipv6 claimed-route [<i>ipv6-source-address</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the number of IPv6 PIM control messages.	display pim ipv6 control-message counters [message-type { probe register register-stop } [interface <i>interface-type interface-number</i> message-type { assert bsr crp graft graft-ack hello join-prune state-refresh }] *] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the DF information of IPv6 BIDIR-PIM.	display pim ipv6 df-info [<i>rp-address</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display information about unacknowledged graft messages.	display pim ipv6 grafts [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the IPv6 PIM information on an interface or all interfaces.	display pim ipv6 interface [<i>interface-type interface-number</i>] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view

Task	Command	Remarks
Display information about join/prune messages to send.	display pim ipv6 join-prune mode { sm [flags <i>flag-value</i>] ssm } [interface <i>interface-type</i> <i>interface-number</i> neighbor <i>ipv6-neighbor-address</i>] * [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv6 PIM neighboring information.	display pim ipv6 neighbor [interface <i>interface-type</i> <i>interface-number</i> <i>ipv6-neighbor-address</i> verbose] * [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display information about the IPv6 PIM routing table.	display pim ipv6 routing-table [<i>ipv6-group-address</i> [<i>prefix-length</i>] <i>ipv6-source-address</i> [<i>prefix-length</i>] incoming-interface [<i>interface-type</i> <i>interface-number</i> register] outgoing-interface { include exclude match } { <i>interface-type</i> <i>interface-number</i> register } mode <i>mode-type</i> flags <i>flag-value</i> fsm] * [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the RP information.	display pim ipv6 rp-info [<i>ipv6-group-address</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Reset IPv6 PIM control message counters.	reset pim ipv6 control-message counters [interface <i>interface-type</i> <i>interface-number</i>]	Available in user view

IPv6 PIM configuration examples

IPv6 PIM-DM configuration example

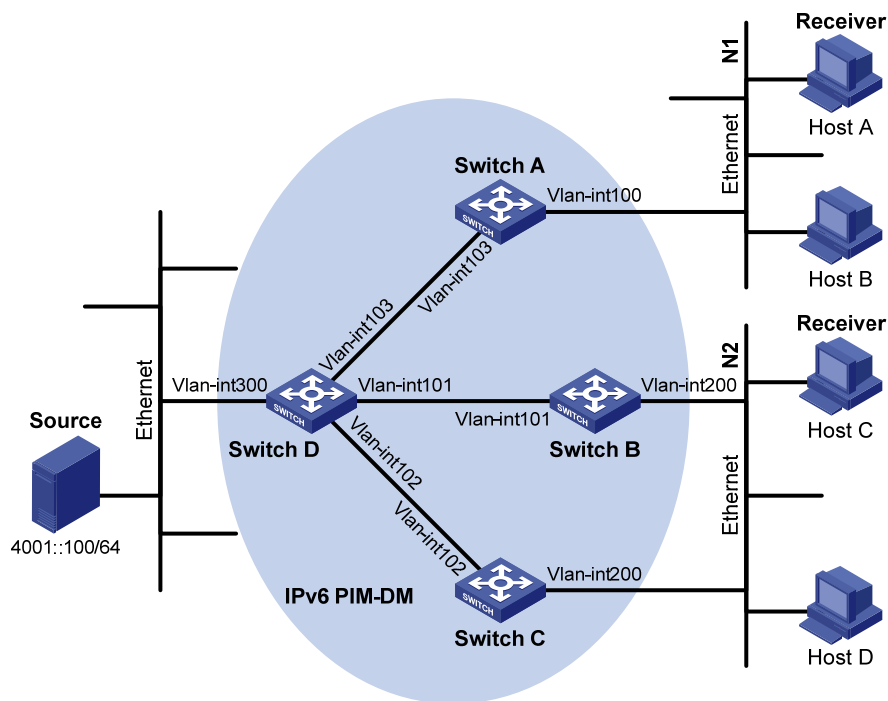
Network requirements

Receivers receive VOD information through multicast. The receiver groups of different organizations form stub networks, and one or more receiver hosts exist in each stub network. The entire IPv6 PIM domain is operating in the dense mode.

Host A and Host C are multicast receivers in two stub networks N1 and N2.

MLDv1 runs between Switch A and N1 and between Switch B/Switch C and N2.

Figure 105 Network diagram



Device	Interface	IPv6 address	Device	Interface	IPv6 address
Switch A	Vlan-int100	1001::1/64	Switch D	Vlan-int300	4001::1/64
	Vlan-int103	1002::1/64		Vlan-int103	1002::2/64
Switch B	Vlan-int200	2001::1/64		Vlan-int101	2002::2/64
	Vlan-int101	2002::1/64		Vlan-int102	3001::2/64
Switch C	Vlan-int200	2001::2/64			
	Vlan-int102	3001::1/64			

Configuration procedure

1. Enable IPv6 forwarding on each switch and configure the IPv6 address and prefix length for each interface as per Figure 105. (Details not shown.)
2. Configure OSPFv3 on the switches in the IPv6 PIM-DM domain to make sure the switches are interoperable at the network layer. (Details not shown.)
3. Enable IPv6 multicast routing, MLD and IPv6 PIM-DM:

Enable IPv6 multicast routing on Switch A, enable MLD on VLAN-interface 100, and enable IPv6 PIM-DM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] pim ipv6 dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim ipv6 dm
[SwitchA-Vlan-interface103] quit
```

Enable IPv6 multicast routing, MLD and IPv6 PIM-DM on Switch B and Switch C in the same way.
(Details not shown.)

Enable IPv6 multicast routing on Switch D, and enable IPv6 PIM-DM on each interface.

```
<SwitchD> system-view
[SwitchD] multicast ipv6 routing-enable
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] pim ipv6 dm
[SwitchD-Vlan-interface300] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim ipv6 dm
[SwitchD-Vlan-interface103] quit
[SwitchD] interface vlan-interface 101
[SwitchD-Vlan-interface101] pim ipv6 dm
[SwitchD-Vlan-interface101] quit
[SwitchD] interface vlan-interface 102
[SwitchD-Vlan-interface102] pim ipv6 dm
[SwitchD-Vlan-interface102] quit
```

Verifying the configuration

Display IPv6 PIM information on Switch D.

```
[SwitchD] display pim ipv6 interface
```

Interface	NbrCnt	HelloInt	DR-Pri	DR-Address
Vlan300	0	30	1	FE80::A01:201:1 (local)
Vlan103	0	30	1	FE80::A01:201:2 (local)
Vlan101	1	30	1	FE80::A01:201:3 (local)
Vlan102	1	30	1	FE80::A01:201:4 (local)

Display IPv6 PIM neighboring relationships on Switch D.

```
[SwitchD] display pim ipv6 neighbor
```

Total Number of Neighbors = 3

Neighbor	Interface	Uptime	Expires	Dr-Priority
FE80::A01:101:1	Vlan103	00:04:00	00:01:29	1
FE80::B01:102:2	Vlan101	00:04:16	00:01:29	3
FE80::C01:103:3	Vlan102	00:03:54	00:01:17	5

Assume that Host A needs to receive the information addressed to IPv6 multicast group G FF0E::101. After IPv6 multicast source S 4001::100/64 sends IPv6 multicast packets to the IPv6 multicast group G, an SPT is established through traffic flooding. Switches on the SPT path (Switch A and Switch D) have their (S, G) entries. Host A sends an MLD report to Switch A to join IPv6 multicast group G, and a (*, G) entry is generated on Switch A. You can use the **display pim IPv6 routing-table** command to view the IPv6 PIM routing table information on each switch. For example:

Display IPv6 PIM multicast routing table information on Switch A.

```

[SwitchA] display pim ipv6 routing-table
Total 1 (*, G) entry; 1 (S, G) entry

(*, FF0E::101)
  Protocol: pim-dm, Flag: WC
  UpTime: 00:01:24
  Upstream interface: NULL
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface100
      Protocol: mld, UpTime: 00:01:20, Expires: never

(4001::100, FF0E::101)
  Protocol: pim-dm, Flag: ACT
  UpTime: 00:01:20
  Upstream interface: Vlan-interface103
    Upstream neighbor: 1002::2
    RPF prime neighbor: 1002::2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface100
      Protocol: pim-dm, UpTime: 00:01:20, Expires: never

```

Display IPv6 PIM multicast routing table information on Switch D.

```

[SwitchD] display pim ipv6 routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(4001::100, FF0E::101)
  Protocol: pim-dm, Flag: LOC ACT
  UpTime: 00:02:19
  Upstream interface: Vlan-interface300
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 2
    1: Vlan-interface103
      Protocol: pim-dm, UpTime: 00:02:19, Expires: never
    2: Vlan-interface102
      Protocol: pim-dm, UpTime: 00:02:19, Expires: never

```

IPv6 PIM-SM non-scoped zone configuration example

Network requirements

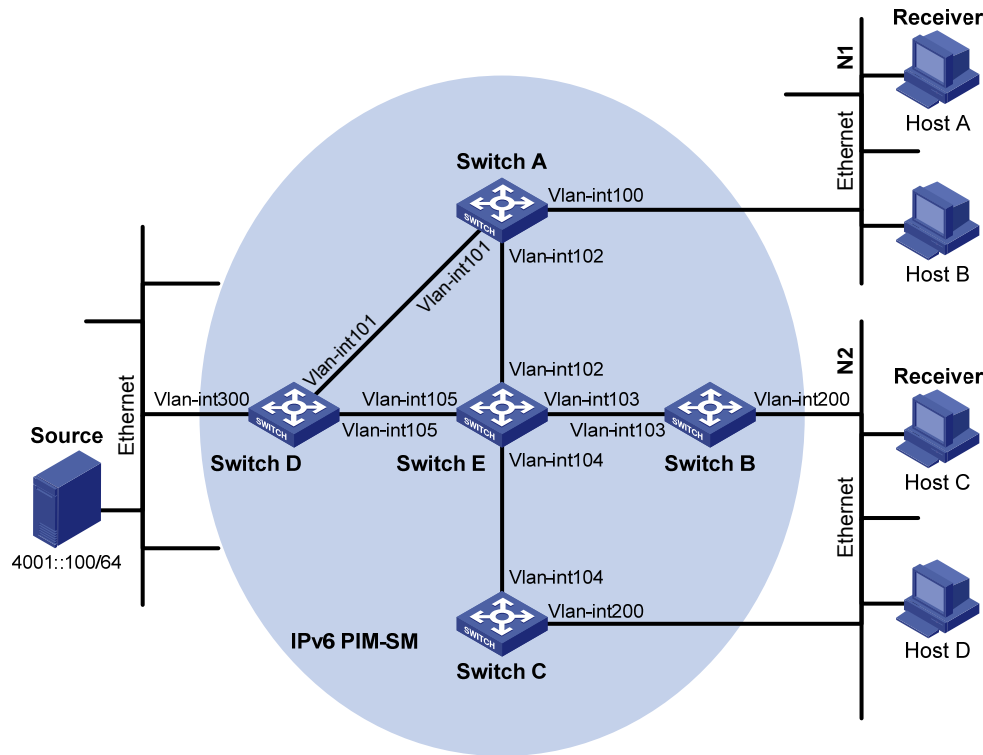
Receivers receive VOD information through multicast. The receiver groups of different organizations form stub networks, and one or more receiver hosts exist in each stub network. The entire PIM domain is operating in the sparse mode.

Host A and Host C are IPv6 multicast receivers in two stub networks, N1 and N2.

VLAN-interface 105 on Switch D and VLAN-interface 102 on Switch E act as C-BSRs and C-RPs. The C-BSR on Switch E has a higher priority. The IPv6 multicast group range to which the C-RP is designated is FFOE::101/64. Modify the hash mask length to map a certain number of consecutive IPv6 group addresses within the range to the two C-RPs.

MLDv1 runs between Switch A and N1 and between Switch B/Switch C and N2.

Figure 106 Network diagram



Device	Interface	IPv6 address	Device	Interface	IPv6 address
Switch A	Vlan-int100	1001::1/64	Switch D	Vlan-int300	4001::1/64
	Vlan-int101	1002::1/64		Vlan-int101	1002::2/64
	Vlan-int102	1003::1/64		Vlan-int105	4002::1/64
Switch B	Vlan-int200	2001::1/64	Switch E	Vlan-int104	3001::2/64
	Vlan-int103	2002::1/64		Vlan-int103	2002::2/64
Switch C	Vlan-int200	2001::2/64		Vlan-int102	1003::2/64
	Vlan-int104	3001::1/64		Vlan-int105	4002::2/64

Configuration procedure

1. Enable IPv6 forwarding on each switch and configure the IPv6 address and prefix length for each interface as per [Figure 106](#). (Details not shown.)
2. Configure OSPFv3 on the switches in the IPv6 PIM-SM domain to make sure the switches are interoperable at the network layer. (Details not shown.)
3. Enable IPv6 multicast routing, MLD and IPv6 PIM-SM

Enable IPv6 multicast routing on Switch A, enable MLD on VLAN-interface 300, and enable IPv6 PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim ipv6 sm
[SwitchA-Vlan-interface102] quit
```

Enable IPv6 multicast routing, MLD and IPv6 PIM-SM on Switch B and Switch C in the same way (Details not shown.).

Enable IPv6 multicast routing and IPv6 PIM-SM on Switch D and Switch E in the same way (Details not shown.).

4. Configure a C-BSR and a C-RP:

On Switch D, configure the service scope of RP advertisements, specify a C-BSR and a C-RP, and set the hash mask length to 128 and the priority of the C-BSR to 10.

```
<SwitchD> system-view
[SwitchD] acl ipv6 number 2005
[SwitchD-acl6-basic-2005] rule permit source ff0e::101 64
[SwitchD-acl6-basic-2005] quit
[SwitchD] pim ipv6
[SwitchD-pim6] c-bsr 4002::1 128 10
[SwitchD-pim6] c-rp 4002::1 group-policy 2005
[SwitchD-pim6] quit
```

On Switch E, configure the service scope of RP advertisements, specify a C-BSR and a C-RP, and set the hash mask length to 128 and the priority of the C-BSR to 20.

```
<SwitchE> system-view
[SwitchE] acl ipv6 number 2005
[SwitchE-acl6-basic-2005] rule permit source ff0e::101 64
[SwitchE-acl6-basic-2005] quit
[SwitchE] pim ipv6
[SwitchE-pim6] c-bsr 1003::2 128 20
[SwitchE-pim6] c-rp 1003::2 group-policy 2005
[SwitchE-pim6] quit
```

Verifying the configuration

Display IPv6 PIM information on all interfaces of Switch A.

```
[SwitchA] display pim ipv6 interface
```

Interface	NbrCnt	HelloInt	DR-Pri	DR-Address
Vlan100	0	30	1	FE80::A01:201:1 (local)

```
Vlan101          1      30      1      FE80::A01:201:2
Vlan102          1      30      1      FE80::A01:201:3
```

Display information about the BSR and locally configured C-RP in effect on Switch A.

```
[SwitchA] display pim ipv6 bsr-info
Elected BSR Address: 1003::2
  Priority: 20
  Hash mask length: 128
  State: Accept Preferred
  Uptime: 00:04:22
  Expires: 00:01:46
```

Display information about the BSR and locally configured C-RP in effect on Switch D.

```
[SwitchD] display pim ipv6 bsr-info
Elected BSR Address: 1003::2
  Priority: 20
  Hash mask length: 128
  State: Elected
  Uptime: 00:05:26
  Expires: 00:01:45
Candidate BSR Address: 4002::1
  Priority: 10
  Hash mask length: 128
  State: Candidate

Candidate RP: 4002::1(Vlan-interface105)
  Priority: 192
  HoldTime: 130
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:48
```

Display information about the BSR and locally configured C-RP in effect on Switch E.

```
[SwitchE] display pim ipv6 bsr-info
Elected BSR Address: 1003::2
  Priority: 20
  Hash mask length: 128
  State: Elected
  Uptime: 00:01:10
  Next BSR message scheduled at: 00:01:48
Candidate BSR Address: 1003::2
  Priority: 20
  Hash mask length: 128
  State: Elected

Candidate RP: 1003::2(Vlan-interface102)
  Priority: 192
  HoldTime: 130
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:48
```

Display RP information on Switch A.

```
[SwitchA] display pim ipv6 rp-info
PIM-SM BSR RP information:
prefix/prefix length: FF0E::101/64
  RP: 4002::1
    Priority: 192
    HoldTime: 130
    Uptime: 00:05:19
    Expires: 00:02:11

  RP: 1003::2
    Priority: 192
    HoldTime: 130
    Uptime: 00:05:19
    Expires: 00:02:11
```

Assume that Host A needs to receive information addressed to the IPv6 multicast group G FF0E::100. The RP corresponding to the multicast group G is Switch E as a result of hash calculation, so an RPT will be built between Switch A and Switch E. When the IPv6 multicast source S 4001::100/64 registers with the RP, an SPT will be built between Switch D and Switch E. After receiving IPv6 multicast data, Switch A immediately switches from the RPT to the SPT. The switches on the RPT path (Switch A and Switch E) have a (*, G) entry, and the switches on the SPT path (Switch A and Switch D) have an (S, G) entry. You can use the **display pim ipv6 routing-table** command to view the PIM routing table information on the switches. For example:

Display IPv6 PIM multicast routing table information on Switch A.

```
[SwitchA] display pim ipv6 routing-table
Total 1 (*, G) entry; 1 (S, G) entry

(*, FF0E::100)
  RP: 1003::2
  Protocol: pim-sm, Flag: WC
  UpTime: 00:03:45
  Upstream interface: Vlan-interface102
    Upstream neighbor: 1003::2
    RPF prime neighbor: 1003::2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface100
      Protocol: mld, UpTime: 00:02:15, Expires: 00:03:06

(4001::100, FF0E::100)
  RP: 1003::2
  Protocol: pim-sm, Flag: SPT ACT
  UpTime: 00:02:15
  Upstream interface: Vlan-interface101
    Upstream neighbor: 1002::2
    RPF prime neighbor: 1002::2
```

```

Downstream interface(s) information:
Total number of downstreams: 1
  1: Vlan-interface100
      Protocol: pim-sm, UpTime: 00:02:15, Expires: 00:03:06

# Display IPv6 PIM multicast routing table information on Switch D.
[SwitchD] display pim ipv6 routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(4001::100, FF0E::100)
  RP: 1003::2
  Protocol: pim-sm, Flag: SPT LOC ACT
  UpTime: 00:14:44
  Upstream interface: Vlan-interface300
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface105
        Protocol: mld, UpTime: 00:14:44, Expires: 00:02:26

# Display IPv6 PIM multicast routing table information on Switch E.
[SwitchE] display pim ipv6 routing-table
Total 1 (*, G) entry; 0 (S, G) entry

(*, FF0E::100)
  RP: 1003::2 (local)
  Protocol: pim-sm, Flag: WC
  UpTime: 00:16:56
  Upstream interface: Register
    Upstream neighbor: 4002::1
    RPF prime neighbor: 4002::1
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface102
        Protocol: pim-sm, UpTime: 00:16:56, Expires: 00:02:34

```

IPv6 PIM-SM admin-scope zone configuration example

Network requirements

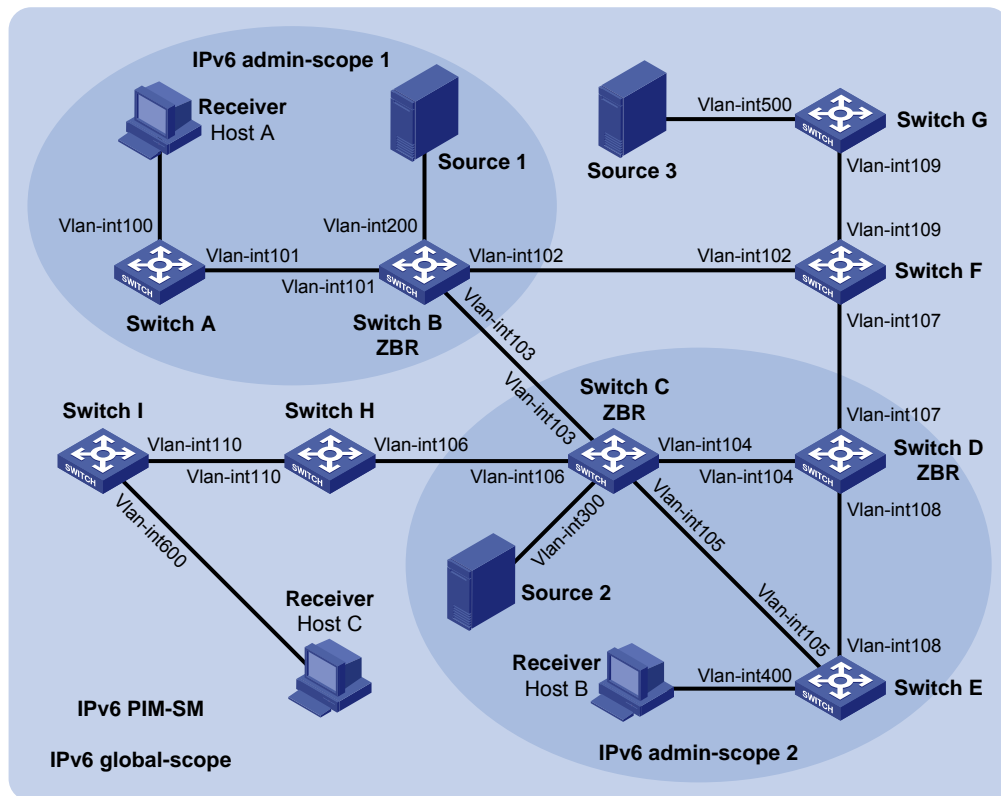
Receivers receive VOD information through multicast. The entire IPv6 PIM-SM domain is divided into IPv6 admin-scope zone 1, IPv6 admin-scope zone 2, and the IPv6 global zone. Switch B, Switch C, and Switch D are ZBRs of these three domains respectively.

Source 1 and Source 2 send different multicast information to FF14::101. Host A receives the multicast information only from Source 1, and Host B receives the multicast information only from Source 2. Source 3 sends multicast information to multicast group FF1E::202. Host C is a multicast receiver for this multicast group.

VLAN-interface 101 of Switch B acts as a C-BSR and C-RP of admin-scope zone 1, which provides services for the IPv6 multicast groups with the Scope field value in their group addresses being 4. VLAN-interface 104 of Switch D acts as a C-BSR and C-RP of admin-scope zone 2, which also provides services for the IPv6 multicast groups with the Scope field value in their group addresses being 4. VLAN-interface 109 of Switch F acts as C-BSRs and C-RPs of the global scope zone, which provides services for IPv6 multicast groups with the Scope field value in their group addresses being 14.

MLDv1 runs between Switch A, Switch E, Switch I, and their respective receivers.

Figure 107 Network diagram



Device	Interface	IPv6 address	Device	Interface	IPv6 address
Switch A	Vlan-int100	1001::1/64	Switch D	Vlan-int104	3002::2/64
	Vlan-int101	1002::1/64		Vlan-int108	6001::1/64
Switch B	Vlan-int200	2001::1/64	Switch E	Vlan-int400	7001::1/64
	Vlan-int101	1002::2/64		Vlan-int105	3003::2/64
	Vlan-int103	2002::1/64	Switch F	Vlan-int108	6001::2/64
	Vlan-int102	2003::1/64		Vlan-int102	2003::2/64
Switch C	Vlan-int300	3001::1/64	Switch G	Vlan-int500	9001::1/64
	Vlan-int104	3002::1/64		Vlan-int109	8001::2/64
	Vlan-int105	3003::1/64	Source 1		—
	Vlan-int103	2002::2/64		Source 2	—
Switch H	Vlan-int110	4001::1/64	Source 3		—
	Vlan-int106	3004::2/64			
Switch I	Vlan-int600	5001::1/64			
	Vlan-int110	4001::2/64			

Configuration procedure

1. Configure the IPv6 address and prefix length for each interface as per Figure 107. (Details not shown.)
2. Configure OSPFv3 on the switches in the IPv6 PIM-SM domain to make sure the switches are interoperable at the network layer. (Details not shown.)

3. Enable IPv6 multicast routing and IPv6 administrative scoping, and enable IPv6 PIM-SM and MLD:

Enable IPv6 multicast routing and administrative scoping on Switch A, enable MLD on the host-side interface VLAN-interface 100, and enable IPv6 PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] pim ipv6
[SwitchA-pim6] c-bsr admin-scope
[SwitchA-pim6] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
```

Enable IPv6 multicast routing and administrative scoping, enable MLD and IPv6 PIM-SM on Switch E and Switch I in the same way. (Details not shown.)

On Switch B, enable IPv6 multicast routing and IPv6 administrative scoping, and enable IPv6 PIM-SM on each interface.

```
<SwitchB> system-view
[SwitchB] multicast ipv6 routing-enable
[SwitchB] pim ipv6
[SwitchB-pim6] c-bsr admin-scope
[SwitchB-pim6] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] pim ipv6 sm
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim ipv6 sm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim ipv6 sm
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] pim ipv6 sm
[SwitchB-Vlan-interface103] quit
```

Enable IPv6 multicast routing and IPv6 administrative scoping, and enable IPv6 PIM-SM on Switch C, Switch D, Switch F, Switch G, and Switch H in the same way. (Details not shown.)

4. Configure an admin-scope zone boundary:

On Switch B, configure VLAN-interface 102 and VLAN-interface 103 to be the boundary of admin-scope zone 1.

```
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] multicast ipv6 boundary scope 4
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 103
```

```
[SwitchB-Vlan-interface103] multicast ipv6 boundary scope 4
[SwitchB-Vlan-interface103] quit
```

On Switch C, configure VLAN-interface 103 and VLAN-interface 106 to be the boundary of admin-scope zone 2.

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 103
[SwitchC-Vlan-interface103] multicast ipv6 boundary scope 4
[SwitchC-Vlan-interface103] quit
[SwitchC] interface vlan-interface 106
[SwitchC-Vlan-interface106] multicast ipv6 boundary scope 4
[SwitchC-Vlan-interface106] quit
```

On Switch D, configure VLAN-interface 107 to be the boundary of admin-scope zone 2.

```
<SwitchD> system-view
[SwitchD] interface vlan-interface 107
[SwitchD-Vlan-interface107] multicast ipv6 boundary scope 4
[SwitchD-Vlan-interface107] quit
```

5. Configure C-BSRs and C-RPs:

On Switch B, configure the service scope of RP advertisements, and configure VLAN-interface 101 as a C-BSR and C-RP of admin-scope zone 1.

```
[SwitchB] pim ipv6
[SwitchB-pim6] c-bsr scope 4
[SwitchB-pim6] c-bsr 1002::2
[SwitchB-pim6] c-rp 1002::2 scope 4
[SwitchB-pim6] quit
```

On Switch D, configure the service scope of RP advertisements, and configure VLAN-interface 104 as a C-BSR and C-RP of admin-scope zone 2.

```
[SwitchD] pim ipv6
[SwitchD-pim6] c-bsr scope 4
[SwitchD-pim6] c-bsr 3002::2
[SwitchD-pim6] c-rp 3002::2 scope 4
[SwitchD-pim6] quit
```

On Switch F, configure VLAN-interface 109 as a C-BSR and C-RP in the global scope zone.

```
<SwitchF> system-view
[SwitchF] pim ipv6
[SwitchF-pim6] c-bsr scope global
[SwitchF-pim6] c-bsr 8001::1
[SwitchF-pim6] c-rp 8001::1
[SwitchF-pim6] quit
```

Verifying the configuration

Display information about the BSR and locally configured C-RP on Switch B.

```
[SwitchB] display pim ipv6 bsr-info
Elected BSR Address: 8001::1
Priority: 64
Hash mask length: 126
State: Accept Preferred
```

```
Scope: 14
Uptime: 00:01:45
Expires: 00:01:25
Elected BSR Address: 1002::2
Priority: 64
Hash mask length: 126
State: Elected
Scope: 4
Uptime: 00:04:54
Next BSR message scheduled at: 00:00:06
Candidate BSR Address: 1002::2
Priority: 64
Hash mask length: 126
State: Elected
Scope: 4

Candidate RP: 1002::2(Vlan-interface101)
Priority: 192
HoldTime: 130
Advertisement Interval: 60
Next advertisement scheduled at: 00:00:15
```

Display information about the BSR and locally configured C-RP on Switch D.

```
[SwitchD] display pim ipv6 bsr-info
Elected BSR Address: 8001::1
Priority: 64
Hash mask length: 126
State: Accept Preferred
Scope: 14
Uptime: 00:01:45
Expires: 00:01:25
Elected BSR Address: 3002::2
Priority: 64
Hash mask length: 126
State: Elected
Scope: 4
Uptime: 00:03:48
Next BSR message scheduled at: 00:01:12
Candidate BSR Address: 3002::2
Priority: 64
Hash mask length: 126
State: Elected
Scope: 4

Candidate RP: 3002::2(Vlan-interface104)
Priority: 192
HoldTime: 130
Advertisement Interval: 60
Next advertisement scheduled at: 00:00:10
```

Display information about the BSR and locally configured C-RP on Switch F.

```
[SwitchF] display pim ipv6 bsr-info
Elected BSR Address: 8001::1
  Priority: 64
  Hash mask length: 126
  State: Elected
  Scope: 14
  Uptime: 00:01:11
  Next BSR message scheduled at: 00:00:49
Candidate BSR Address: 8001::1
  Priority: 64
  Hash mask length: 126
  State: Elected
  Scope: 14

Candidate RP: 8001::1(Vlan-interface109)
  Priority: 192
  HoldTime: 130
  Advertisement Interval: 60
  Next advertisement scheduled at: 00:00:55
```

To view the RP information learned on a switch, use the **display pim ipv6 rp-info** command. For example:

Display RP information on Switch B.

```
[SwitchB] display pim ipv6 rp-info
PIM-SM BSR RP information:
prefix/prefix length: FF0E::/16
  RP: 8001::1
  Priority: 192
  HoldTime: 130
  Uptime: 00:03:39
  Expires: 00:01:51

prefix/prefix length: FF1E::/16
  RP: 8001::1
  Priority: 192
  HoldTime: 130
  Uptime: 00:03:39
  Expires: 00:01:51

prefix/prefix length: FF2E::/16
  RP: 8001::1
  Priority: 192
  HoldTime: 130
  Uptime: 00:03:39
  Expires: 00:01:51

prefix/prefix length: FF3E::/16
  RP: 8001::1
```

Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF4E::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF5E::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF6E::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF7E::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF8E::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF9E::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFAE::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFBE::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFCE::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFDE::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFEE::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFFE::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF04::/16

RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF14::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF24::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF34::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF44::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF54::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF64::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF74::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF84::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF94::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFA4::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFB4::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFC4::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFD4::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFE4::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39

Expires: 00:01:51

prefix/prefix length: FFF4::/16
RP: 1002::2
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

Display RP information on Switch F.

```
[SwitchF] display pim rp-info  
PIM-SM BSR RP information:  
prefix/prefix length: FF0E::/16  
RP: 8001::1  
Priority: 192  
HoldTime: 130  
Uptime: 00:03:39  
Expires: 00:01:51
```

prefix/prefix length: FF1E::/16
RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF2E::/16
RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF3E::/16
RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF4E::/16
RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF5E::/16
RP: 8001::1

Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF6E::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF7E::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF8E::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FF9E::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFAE::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFBE::/16

RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFCE::/16

```
RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFDE::/16
RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFEE::/16
RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51

prefix/prefix length: FFFE::/16
RP: 8001::1
Priority: 192
HoldTime: 130
Uptime: 00:03:39
Expires: 00:01:51
```

IPv6 BIDIR-PIM configuration example

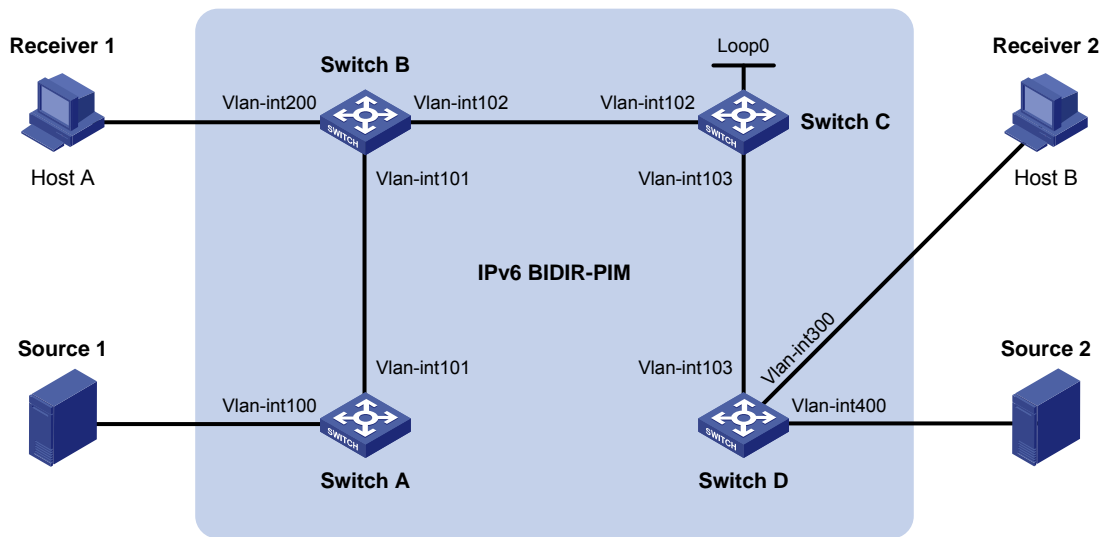
Network requirements

In the IPv6 BIDIR-PIM domain shown in [Figure 108](#). Source 1 and Source 2 send different IPv6 multicast information to IPv6 multicast group FF14::101. Host A and Host B receive IPv6 multicast information from the two sources.

VLAN interface 102 of Switch C acts as a C-BSR, and loopback interface 0 acts as a C-RP of the IPv6 BIDIR-PIM domain.

MLDv1 runs between Switch B and Host A and between Switch D and Host B.

Figure 108 Network diagram



Device	Interface	IPv6 address	Device	Interface	IPv6 address
Switch A	Vlan-int100	1001::1/64	Switch D	Vlan-int300	4001::1/64
	Vlan-int101	1002::1/64		Vlan-int400	5001::1/64
Switch B	Vlan-int200	2001::1/64		Vlan-int103	3001::2/64
	Vlan-int101	1002::2/64	Source 1	-	1001::2/64
	Vlan-int102	2002::1/64	Source 2	-	5001::2/64
Switch C	Vlan-int102	2002::2/64	Receiver 1	-	2001::2/64
	Vlan-int103	3001::1/64	Receiver 2	-	4001::2/64
	Loop0	6001::1/128			

Configuration procedure

1. Enable IPv6 forwarding on each switch, and configure the IPv6 address and prefix length for each interface as per Figure 108. (Details not shown.)
2. Configure OSPFv3 on the switches in the IPv6 BIDIR-PIM domain to make sure the switches are interoperable at the network layer. (Details not shown.)
3. Enable IPv6 multicast routing, IPv6 PIM-SM, IPv6 BIDIR-PIM, and MLD:

On Switch A, enable IPv6 multicast routing, enable IPv6 PIM-SM on each interface, and enable IPv6 BIDIR-PIM.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
[SwitchA] pim ipv6
[SwitchA-pim6] bidir-pim enable
[SwitchA-pim6] quit
```

On Switch B, enable IPv6 multicast routing, enable IPv6 PIM-SM on each interface, enable MLD in VLAN interface 200, and enable IPv6 BIDIR-PIM.

```
<SwitchB> system-view
[SwitchB] multicast ipv6 routing-enable
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] mld enable
[SwitchB-Vlan-interface200] pim ipv6 sm
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim ipv6 sm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim ipv6 sm
[SwitchB-Vlan-interface102] quit
[SwitchB] pim ipv6
[SwitchB-pim6] bidir-pim enable
[SwitchB-pim6] quit
```

On Switch C, enable IPv6 multicast routing, enable IPv6 PIM-SM on each interface, and enable IPv6 BIDIR-PIM.

```
<SwitchC> system-view
[SwitchC] multicast ipv6 routing-enable
[SwitchC] interface vlan-interface 102
[SwitchC-Vlan-interface102] pim ipv6 sm
[SwitchC-Vlan-interface102] quit
[SwitchC] interface vlan-interface 103
[SwitchC-Vlan-interface103] pim ipv6 sm
[SwitchC-Vlan-interface103] quit
[SwitchC] interface loopback 0
[SwitchC-LoopBack0] pim ipv6 sm
[SwitchC-LoopBack0] quit
[SwitchC] pim ipv6
[SwitchC-pim6] bidir-pim enable
```

On Switch D, enable IPv6 multicast routing, enable IPv6 PIM-SM on each interface, enable MLD in VLAN interface 300, and enable IPv6 BIDIR-PIM.

```
<SwitchD> system-view
[SwitchD] multicast ipv6 routing-enable
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] mld enable
[SwitchD-Vlan-interface300] pim ipv6 sm
[SwitchD-Vlan-interface300] quit
[SwitchD] interface vlan-interface 400
[SwitchD-Vlan-interface400] pim ipv6 sm
[SwitchD-Vlan-interface400] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim ipv6 sm
[SwitchD-Vlan-interface103] quit
[SwitchD] pim ipv6
```

```
[SwitchD-pim6] bidir-pim enable
[SwitchD-pim6] quit
```

4. On Switch C, configure VLAN interface 102 as a C-BSR, and loopback interface 0 as a C-RP for the entire IPv6 BIDIR-PIM domain.

```
[SwitchC-pim6] c-bsr 2002::2
[SwitchC-pim6] c-rp 6001::1 bidir
[SwitchC-pim6] quit
```

Verifying the configuration

Display the DF information of IPv6 BIDIR-PIM on Switch A.

```
[SwitchA] display pim ipv6 df-info
RP Address: 6001::1
```

Interface	State	DF-Pref	DF-Metric	DF-Uptime	DF-Address
Vlan100	Win	100	2	01:08:50	FE80::200:5EFF: FE71:2800 (local)
Vlan101	Lose	100	1	01:07:49	FE80::20F:E2FF: FE38:4E01

Display the DF information of IPv6 BIDIR-PIM on Switch B.

```
[SwitchB] display pim ipv6 df-info
RP Address: 6001::1
```

Interface	State	DF-Pref	DF-Metric	DF-Uptime	DF-Address
Vlan200	Win	100	1	01:24:09	FE80::200:5EFF: FE71:2801 (local)
Vlan101	Win	100	1	01:24:09	FE80::20F:E2FF: FE38:4E01 (local)
Vlan102	Lose	0	0	01:23:12	FE80::20F:E2FF: FE15:5601

Display the DF information of IPv6 BIDIR-PIM on Switch C.

```
[SwitchC] display pim ipv6 df-info
RP Address: 6001::1
```

Interface	State	DF-Pref	DF-Metric	DF-Uptime	DF-Address
Loop0	-	-	-	-	-
Vlan102	Win	0	0	01:06:07	FE80::20F:E2FF: FE15:5601 (local)
Vlan103	Win	0	0	01:06:07	FE80::20F:E2FF: FE15:5602 (local)

Display the DF information of IPv6 BIDIR-PIM on Switch D.

```
[SwitchD] display pim ipv6 df-info
RP Address: 6001::1
```

Interface	State	DF-Pref	DF-Metric	DF-Uptime	DF-Address
Vlan300	Win	100	1	01:19:53	FE80::200:5EFF: FE71:2803 (local)
Vlan400	Win	100	1	00:39:34	FE80::200:5EFF: FE71:2802 (local)
Vlan103	Lose	0	0	01:21:40	FE80::20F:E2FF: FE15:5602

Display the DF information of the IPv6 multicast forwarding table on Switch A.

```
[SwitchA] display multicast ipv6 forwarding-table df-info
Multicast DF information
Total 1 RP
```

Total 1 RP matched

```
00001. RP Address: 6001::1
  MID: 0, Flags: 0x2100000:0
  Uptime: 00:08:32
  RPF interface: Vlan-interface101
  List of 1 DF interfaces:
    1: Vlan-interface100
```

Display the DF information of the IPv6 multicast forwarding table on Switch B.

```
[SwitchB] display multicast ipv6 forwarding-table df-info
Multicast DF information
Total 1 RP
```

Total 1 RP matched

```
00001. RP Address: 6001::1
  MID: 0, Flags: 0x2100000:0
  Uptime: 00:06:24
  RPF interface: Vlan-interface102
  List of 2 DF interfaces:
    1: Vlan-interface101
    2: Vlan-interface200
```

Display the DF information of the IPv6 multicast forwarding table on Switch C.

```
[SwitchC] display multicast ipv6 forwarding-table df-info
Multicast DF information
Total 1 RP
```

Total 1 RP matched

```
00001. RP Address: 6001::1
  MID: 0, Flags: 0x2100000:0
  Uptime: 00:07:21
  RPF interface: LoopBack0
  List of 2 DF interfaces:
    1: Vlan-interface102
    2: Vlan-interface103
```

Display the DF information of the IPv6 multicast forwarding table on Switch D.

```
[SwitchD] display multicast ipv6 forwarding-table df-info
Multicast DF information
Total 1 RP
```

Total 1 RP matched

```

00001. RP Address: 6001::1
MID: 0, Flags: 0x2100000:0
Uptime: 00:05:12
RPF interface: Vlan-interface103
List of 2 DF interfaces:
  1: Vlan-interface300
  2: Vlan-interface400

```

IPv6 PIM-SSM configuration example

Network requirements

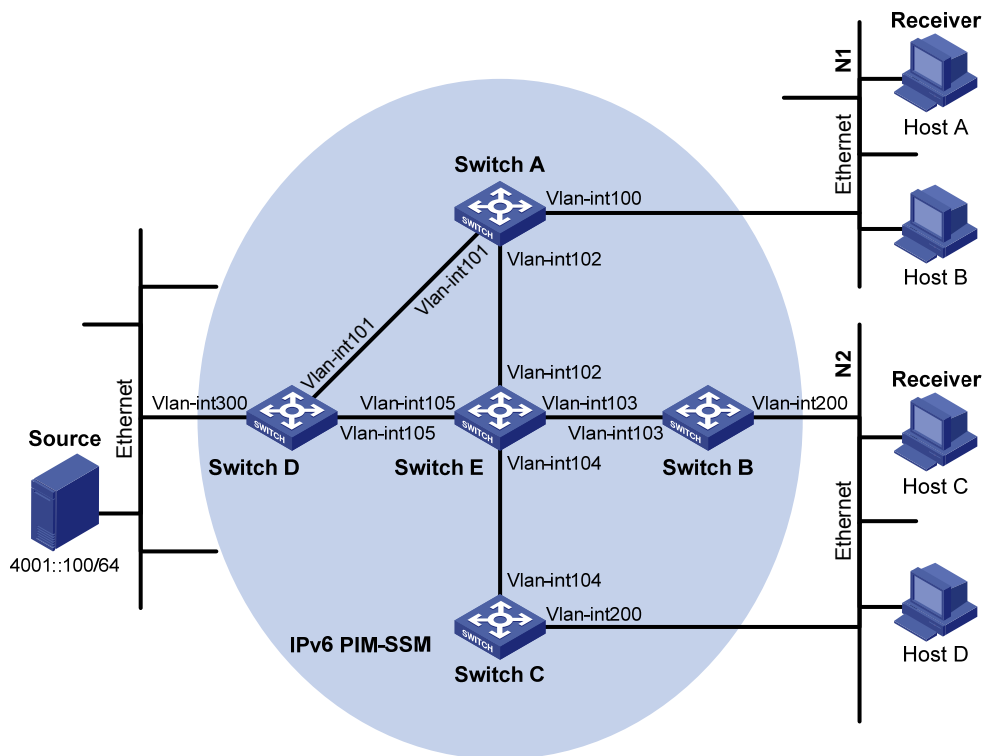
Receivers receive VOD information through multicast. The receiver groups of different organizations form stub networks, and one or more receiver hosts exist in each stub network. The entire PIM domain is operating in the SSM mode.

Host A and Host C are IPv6 multicast receivers in two stub networks, N1 and N2.

The SSM group range is FF3E::/64.

MLDv2 runs between Switch A and N1 and between Switch B/Switch C and N2.

Figure 109 Network diagram



Device	Interface	IPv6 address	Device	Interface	IPv6 address
Switch A	Vlan-int100	1001::1/64	Switch D	Vlan-int300	4001::1/64
	Vlan-int101	1002::1/64		Vlan-int101	1002::2/64

	Vlan-int102	1003::1/64		Vlan-int105	4002::1/64
Switch B	Vlan-int200	2001::1/64	Switch E	Vlan-int104	3001::2/64
	Vlan-int103	2002::1/64		Vlan-int103	2002::2/64
Switch C	Vlan-int200	2001::2/64		Vlan-int102	1003::2/64
	Vlan-int104	3001::1/64		Vlan-int105	4002::2/64

Configuration procedure

1. Enable IPv6 forwarding on each switch and configure the IPv6 address and prefix length for each interface as per [Figure 109](#). (Details not shown.)
2. Configure OSPFv3 on the switches in the IPv6 PIM-SSM domain to make sure the switches are interoperable at the network layer. (Details not shown.)
3. Enable IPv6 multicast routing, MLD and IPv6 PIM-SM:

Enable IPv6 multicast routing on Switch A, enable MLDv2 on VLAN-interface 100, and enable IPv6 PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] mld version 2
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim ipv6 sm
[SwitchA-Vlan-interface102] quit
```

Enable IPv6 multicast routing, MLD and IPv6 PIM-SM on Switch B and Switch C is similar to that on Switch A in the same way. (Details not shown.)

Enable IPv6 multicast routing and IPv6 PIM-SM on Switch D and Switch E in the same way. (Details not shown.)

4. Configure the IPv6 SSM group range:

Configure the IPv6 SSM group range to be FF3E::/64 on Switch A.

```
[SwitchA] acl ipv6 number 2000
[SwitchA-acl6-basic-2000] rule permit source ff3e:: 64
[SwitchA-acl6-basic-2000] quit
[SwitchA] pim ipv6
[SwitchA-pim6] ssm-policy 2000
[SwitchA-pim6] quit
```

Configure the IPv6 SSM group range on Switch B, Switch C, Switch D, and Switch E in the same way. (Details not shown.)

Verifying the configuration

Display IPv6 PIM information on Switch A.

```
[SwitchA] display pim ipv6 interface
Interface          NbrCnt HelloInt  DR-Pri  DR-Address
Vlan100            0       30        1       FE80::A01:201:1
                  (local)
Vlan101            1       30        1       FE80::A01:201:2
Vlan102            1       30        1       FE80::A01:201:3
```

Assume that Host A needs to receive the information a specific IPv6 multicast source S 4001::100/64 sends to IPv6 multicast group G FF3E::101. Switch A builds an SPT toward the IPv6 multicast source. Switches on the SPT path (Switch A and Switch D) have generated an (S, G) entry, but Switch E, which is not on the SPT path, does not have IPv6 multicast routing entries. You can use the **display pim ipv6 routing-table** command to view the IPv6 PIM routing table information on each switch. For example:

Display IPv6 PIM multicast routing table information on Switch A.

```
[SwitchA] display pim ipv6 routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(4001::100, FF3E::101)
  Protocol: pim-ssm, Flag:
  UpTime: 00:00:11
  Upstream interface: Vlan-interface101
    Upstream neighbor: 1002::2
    RPF prime neighbor: 1002::2
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface100
      Protocol: mld, UpTime: 00:00:11, Expires: 00:03:25
```

Display IPv6 PIM multicast routing table information on Switch B.

```
[SwitchD] display pim ipv6 routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(4001::100, FF3E::101)
  Protocol: pim-ssm, Flag: LOC
  UpTime: 00:08:02
  Upstream interface: Vlan-interface300
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
  Total number of downstreams: 1
    1: Vlan-interface105
      Protocol: pim-ssm, UpTime: 00:08:02, Expires: 00:03:25
```

Troubleshooting IPv6 PIM configuration

Failure to build a multicast distribution tree correctly

Symptom

None of the routers in the network (including routers directly connected with IPv6 multicast sources and receivers) have IPv6 multicast forwarding entries. That is, a multicast distribution tree cannot be built correctly and clients cannot receive IPv6 multicast data.

Analysis

- An IPv6 PIM routing entry is created based on an IPv6 unicast route, whichever IPv6 PIM mode is running. Multicast works only when unicast does.
- IPv6 PIM must be enabled on the RPF interface. An RPF neighbor must be an IPv6 PIM neighbor as well. If IPv6 PIM is not enabled on the RPF interface or the RPF neighbor, the establishment of a multicast distribution tree will fail, resulting in abnormal multicast forwarding.
- IPv6 PIM requires that the same IPv6 PIM mode (namely, DM or SM) must run on the entire network. Otherwise, the establishment of a multicast distribution tree will fail, resulting in abnormal multicast forwarding.

Solution

1. Use the **display ipv6 routing-table** command to verify that a unicast route exists to the IPv6 multicast source or the RP.
2. Use the **display pim ipv6 interface** command to verify that the RPF interface is IPv6 PIM enabled. If IPv6 PIM is not enabled on the interface, use the **pim ipv6 dm** or **pim ipv6 sm** command to enable IPv6 PIM.
3. Use the **display pim ipv6 neighbor** command to verify that the RPF neighbor is an IPv6 PIM neighbor.
4. Verify that IPv6 PIM and MLD are enabled on the interfaces that are directly connected to the IPv6 multicast source and to the receiver.
5. Use the **display pim ipv6 interface verbose** command to verify that the same PIM mode is enabled on the RPF interface and the corresponding interface of the RPF neighbor router.
6. Use the **display current-configuration** command to verify that the same IPv6 PIM mode is enabled on all the routers in the entire network. Make sure that the same IPv6 PIM mode is enabled on all the routers: IPv6 PIM-SM on all routers, or IPv6 PIM-DM on all routers.

IPv6 multicast data abnormally terminated on an intermediate router

Symptom

An intermediate router can receive IPv6 multicast data successfully, but the data cannot reach the last hop router. An interface on the intermediate router receives data, but no corresponding (S, G) entry is created in the IPv6 PIM routing table.

Analysis

- If an IPv6 multicast forwarding boundary has been configured through the **multicast ipv6 boundary** command, any IPv6 multicast packet will be kept from crossing the boundary, and no routing entry can be created in the IPv6 PIM routing table.
- In addition, the **source-policy** command filters received IPv6 multicast packets. If the IPv6 multicast data fails to pass the IPv6 ACL rule defined in this command, IPv6 PIM cannot create the route entry either.

Solution

1. Use the **display current-configuration** command to verify the IPv6 multicast forwarding boundary settings. Use the **multicast ipv6 boundary** command to change the IPv6 multicast forwarding boundary settings.
2. Use the **display current-configuration** command to verify the IPv6 multicast filter configuration. Change the IPv6 ACL rule defined in the **source-policy** command so that the source/group address of the IPv6 multicast data can pass ACL filtering.

RPS cannot join SPT in IPv6 PIM-SM

Symptom

An RPT cannot be established correctly, or the RPs cannot join the SPT to the IPv6 multicast source.

Analysis

- As the core of an IPv6 PIM-SM domain, the RPs provide services for specific IPv6 multicast groups. Multiple RPs can coexist in a network. Make sure that the RP information on all routers is exactly the same and that a specific group is mapped to the same RP. Otherwise, IPv6 multicast will fail.
- In the case of the static RP mechanism, the same RP address must be configured on all the routers in the entire network, including static RPs, by means of the static RP command. Otherwise, IPv6 multicast will fail.

Solution

1. Use the **display ipv6 routing-table** command to verify that a route is available on each router to the RP.

2. Use the **display pim ipv6 rp-info** command to verify that the RP information is consistent on all routers. In the case of inconsistent RP information, configure consistent RP address on all the routers.
3. Use the **display pim ipv6 rp-info** command to verify that the same RP address has been configured on all the routers throughout the network.

RPT establishment failure or source registration failure in IPv6 PIM-SM

Symptom

C-RPs cannot unicast advertise messages to the BSR. The BSR does not advertise bootstrap messages containing C-RP information and has no unicast route to any C-RP. An RPT cannot be established correctly, or the DR cannot perform source registration with the RP.

Analysis

- C-RPs periodically send advertisement messages to the BSR by unicast. If a C-RP does not have a route to the BSR, the BSR cannot receive the advertisements from the C-RP, and the bootstrap messages of the BSR will not contain the information about that C-RP.
- The RP is the core of an IPv6 PIM-SM domain. Make sure that the RP information on all routers is exactly the same, a specific group is mapped to the same RP, and a unicast route is available to the RP.

Solution

1. Use the **display ipv6 routing-table** command to verify that routes are available on each router to the RP and the BSR, and whether a route is available between the RP and the BSR. Make sure that each C-RP has a unicast route to the BSR, the BSR has a unicast route to each C-RP, and all the routers in the entire network have a unicast route to the RP.
2. IPv6 PIM-SM needs the support of the RP and BSR. Use the **display pim ipv6 bsr-info** command to verify that the BSR information is available on each router, and then use the **display pim ipv6 rp-info** command to check whether the RP information is correct.
3. Use the **display pim ipv6 neighbor** command to verify that normal neighboring relationships have been established among the routers.

Configuring IPv6 MBGP (available only on the HP 5500 EI)

This chapter covers configuration tasks related to multiprotocol BGP for IPv6 multicast. For information about BGP and IPv6 BGP, see *Layer 3—IP Routing Configuration Guide*.

The term "router" in this chapter refers to both routers and Layer 3 switches.

IPv6 MBGP overview

IETF defined Multiprotocol BGP (MP-BGP) to carry routing information for multiple network-layer protocols.

For an IPv6 network, the topology for IPv6 multicast might be different from that for IPv6 unicast. To distinguish them, the MP-BGP enables BGP to carry the IPv6 unicast Network Layer Reachability Information (NLRI) and IPv6 multicast NLRI separately, and the multicast NLRI performs reverse path forwarding (RPF) exclusively. In this way, route selection for a destination through the IPv6 unicast routing table and through the IPv6 multicast routing table have different results, ensuring consistent unicast forwarding and normal multicast between domains. For information about RPF, see "[Configuring multicast routing and forwarding \(available only on the HP 5500 EI\)](#)."

MP-BGP is defined in RFC 2858 (Multiprotocol Extensions for BGP-4). The application of MP-BGP on IPv6 multicast is called IPv6 Multicast BGP (IPv6 MBGP).

IPv6 MBGP configuration task list

Task	Remarks
Configuring basic IPv6 MBGP functions	Configuring an IPv6 MBGP peer Required
	Configuring a preferred value for routes from a peer or a peer group Optional
Controlling route distribution and reception	Injecting a local IPv6 MBGP route Optional
	Configuring IPv6 MBGP route redistribution Optional
	Configuring IPv6 MBGP route summarization Optional
	Advertising a default route to a peer or peer group Optional
	Configuring outbound IPv6 MBGP route filtering Optional
	Configuring inbound IPv6 MBGP route filtering Optional
	Configuring IPv6 MBGP route dampening Optional

Task	Remarks	
Configuring IPv6 MBGP route attributes	Configuring IPv6 MBGP route preferences	
	Configuring the default local preference	Optional
	Configuring the MED attribute	
	Configuring the NEXT_HOP attribute	Optional
Tuning and optimizing IPv6 MBGP networks	Configuring the AS_PATH attribute	Optional
	Configuring IPv6 MBGP soft reset	Optional
	Enabling the IPv6 MBGP orf capability	Optional
Configuring a large scale IPv6 MBGP network	Configuring the maximum number of equal-cost routes for load-balancing	Optional
	Configuring an IPv6 MBGP peer group	Optional
	Configuring IPv6 MBGP community	Optional
	Configuring an IPv6 MBGP route reflector	Optional

Configuring basic IPv6 MBGP functions

Configuration prerequisites

IPv6 MBGP is an application of multiprotocol BGP. Before you configure IPv6 MBGP, complete the following tasks:

- Enable IPv6.
- Configure network layer addresses for interfaces.
- Complete BGP basic configuration.

Configuring an IPv6 MBGP peer

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable BGP and enter BGP view.	bgp <i>as-number</i>	Not enabled by default.
3. Enter IPv6 address family view.	ipv6-family	N/A
4. Specify an IPv6 BGP peer and its AS number.	peer <i>ipv6-address</i> as-number <i>as-number</i>	Not configured by default.
5. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
6. Enable the IPv6 MBGP peer.	peer <i>ipv6-address</i> enable	Not enabled by default.

Configuring a preferred value for routes from a peer or a peer group

If you both reference a routing policy and use the command **peer { ipv6-group-name | ipv6-address } preferred-value value** to set a preferred value for routes from a peer or a peer group, the routing policy sets the specified preferred value for the routes that match it. Other routes that do not match the routing policy use the value set through the command. If the preferred value in the routing policy is 0, the routes that match it will also use the value set through the **peer { ipv6-group-name | ipv6-address } preferred-value value** command. To learn how to use a routing policy to set a preferred value, see the **peer { ipv6-group-name | ipv6-address } route-policy route-policy-name { import | export }** command and the **apply preferred-value preferred-value** command. For more information about these commands, see *Layer 3—IP Routing Command Reference*.

To configure a preferred value for routes from a peer or a peer group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp as-number	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Specify a preferred value for routes received from the IPv6 MBGP peer or the peer group.	peer { ipv6-group-name ipv6-address } preferred-value value	Optional. The preferred value defaults to 0.

Controlling route distribution and reception

Configuration prerequisites

Before you configure this task, complete the following tasks:

- Enable IPv6.
- Configure basic IPv6 MBGP functions.

Injecting a local IPv6 MBGP route

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp as-number	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A

Step	Command	Remarks
4. Inject a network into the IPv6 MBGP routing table.	network <i>ipv6-address prefix-length</i> [route-policy <i>route-policy-name</i> short-cut]	Not injected by default.

Configuring IPv6 MBGP route redistribution

Step	Command	Description
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv6 MBGP multicast address family view.	ipv6-family multicast	N/A
4. Enable default route redistribution into the IPv6 MBGP routing table.	default-route imported	Optional. By default, default route redistribution is not allowed. If the default-route imported command is not configured, using the import-route command cannot redistribute any IGP default route.
5. Enable route redistribution from another routing protocol.	import-route <i>protocol</i> [<i>process-id</i> med <i>med-value</i> route-policy <i>route-policy-name</i>] *]	Not enabled by default.

Configuring IPv6 MBGP route summarization

To reduce the routing table size on medium and large BGP networks, you must configure route summarization on IPv6 MBGP routers. BGP supports only manual summarization of IPv6 multicast routes.

To configure IPv6 MBGP route summarization:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Configure manual route summarization.	aggregate <i>ipv6-address prefix-length</i> [as-set attribute-policy <i>route-policy-name</i> detail-suppressed origin-policy <i>route-policy-name</i> suppress-policy <i>route-policy-name</i>]*	Not configured by default.

Advertising a default route to a peer or peer group

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp as-number	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Advertise a default route to an IPv6 MBGP peer or peer group.	peer { ipv6-group-name ipv6-address } default-route-advertise [route-policy route-policy-name]	Not advertised by default. With the peer default-route-advertise command executed, the router sends a default route with the next hop as itself to the specified IPv6 MBGP peer or the specified peer group, regardless of whether the default route is available in the routing table.

Configuring outbound IPv6 MBGP route filtering

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp as-number	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Configure outbound IPv6 MBGP route filtering.	<ul style="list-style-type: none"> Configure the filtering of outgoing routes: filter-policy { acl6-number ipv6-prefix ipv6-prefix-name } export [protocol process-id] Specify an IPv6 ACL to filter routes advertised to a peer or a peer group: peer { ipv6-group-name ipv6-address } filter-policy acl6-number export Specify an AS path list to filter IPv6 MBGP routing information advertised to a peer or a peer group: peer { ipv6-group-name ipv6-address } as-path-acl as-path-acl-number export Specify an IPv6 prefix list to filter routes advertised to a peer or a peer group: peer { ipv6-group-name ipv6-address } ipv6-prefix ipv6-prefix-name export Apply a routing policy to routes advertised to a peer or a peer group: peer { ipv6-group-name ipv6-address } route-policy route-policy-name export 	<p>Use any of the commands.</p> <p>No filtering is configured by default.</p> <p>You can configure filter policies as required. If you configure multiple filter policies, they are applied in the following order:</p> <ol style="list-style-type: none"> filter-policy export peer filter-policy export peer as-path-acl export peer ipv6-prefix export peer route-policy export <p>A filter policy can be applied only after the previous one is passed. Routing information can be advertised only after passing all the configured filter policies.</p>

NOTE:

- Members of an IPv6 MBGP peer group must have the same outbound route filtering policy as the peer group.
 - IPv6 BGP advertises the redistributed routes that pass the specified policy to the IPv6 MBGP peer.
-

Configuring inbound IPv6 MBGP route filtering

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Configure IPv6 MBGP inbound route filtering.	<ul style="list-style-type: none">• Configure inbound route filtering: filter-policy { <i>acl6-number</i> ipv6-prefix <i>ipv6-prefix-name</i> } import• Apply a routing policy to routes from a peer or a peer group: peer { <i>ipv6-group-name</i> <i>ipv6-address</i> } route-policy <i>route-policy-name</i> import• Specify an IPv6 ACL to filter routes from a peer or a peer group: peer { <i>ipv6-group-name</i> <i>ipv6-address</i> } filter-policy <i>acl6-number</i> import• Specify an AS path list to filter IPv6 BGP routing information from a peer or a peer group: peer { <i>ipv6-group-name</i> <i>ipv6-address</i> } as-path-acl <i>as-path-acl-number</i> import• Specify an IPv6 prefix list to filter routes from a peer or a peer group: peer { <i>ipv6-group-name</i> <i>ipv6-address</i> } ipv6-prefix <i>ipv6-prefix-name</i> import	<p>Use any of the commands</p> <p>By default, advertised routes are not filtered.</p> <p>You can configure a filtering policy as required.</p> <p>If you configure several filtering policies, they are applied in the following sequence:</p> <ol style="list-style-type: none">5. filter-policy import6. peer filter-policy import7. peer as-path-acl import8. peer ip-prefix import9. peer route-policy import <p>A filter policy can be applied only after the previous one is passed. Routing information can be received only after passing all the configured filter policies.</p>
10. Specify the upper limit of prefixes that can be imported from a peer or a peer group.	peer { <i>ipv6-group-name</i> <i>ipv6-address</i> } route-limit <i>limit</i> [<i>percentage</i>]	Optional. The number is unlimited by default.

NOTE:

A peer can have an inbound route filtering policy that is different from the policy of the peer group that it belongs to. That is, peer group members can have different inbound route filtering policies.

Configuring IPv6 MBGP route dampening

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Configure IPv6 MBGP route dampening parameters.	dampening [<i>half-life-reachable</i> <i>half-life-unreachable</i> <i>reuse</i> <i>suppress ceiling</i> route-policy <i>route-policy-name</i>]*	Optional. Not configured by default.

Configuring IPv6 MBGP route attributes

This section describes how to use IPv6 MBGP route attributes to affect IPv6 MBGP route selection. IPv6 MBGP route attributes involve:

- IPv6 MBGP protocol preference
- Default LOCAL_PREF attribute
- MED attribute
- NEXT_HOP attribute
- AS_PATH attribute

Configuration prerequisites

Before you configure IPv6 MBGP route attributes, complete the following tasks:

- Enable IPv6.
- Configure basic IPv6 MBGP functions.

Configuring IPv6 MBGP route preferences

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Configure preferences for external, internal, and local IPv6 MBGP routes.	preference { <i>external-preference</i> <i>internal-preference</i> <i>local-preference</i> route-policy <i>route-policy-name</i> }	Optional. The default preference values of external, internal, and local routes are 255, 255, and 130, respectively.

Configuring the default local preference

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Set the default local preference.	default local-preference <i>value</i>	Optional. By default, the default local preference is 100.

Configuring the MED attribute

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Configure a default MED value.	default med <i>med-value</i>	Optional. By default, the default <i>med-value</i> is 0.
5. Enable the comparison of the MED for routes from different ASs.	compare-different-as-med	Optional. Not enabled by default.
6. Enable the comparison of the MED for routes from each AS.	bestroute compare-med	Optional. Disabled by default.
7. Enable the comparison of the MED for routes from confederation peers.	bestroute med-confederation	Optional. Disabled by default.

Configuring the NEXT_HOP attribute

You can use the **peer next-hop-local** command to specify the local router as the next hop of routes sent to an IPv6 multicast IBGP peer or a peer group. If load balancing is configured, the router specifies itself as the next hop of routes sent to the IPv6 multicast IBGP peer or the peer group regardless of whether the **peer next-hop-local** command is configured.

In a third-party next-hop network, that is, the local router has two IPv6 multicast EBGP peers in a broadcast network, the router does not specify itself as the next hop of routes sent to the EBGP peers by default.

To specify the router as the next hop of routes sent to a peer or a peer group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A

Step	Command	Remarks
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Configure the router as the next hop of routes sent to the peer or the peer group.	peer { <i>ipv6-group-name</i> <i>ipv6-address</i> } next-hop-local	Optional. By default, IPv6 MBGP specifies the local router as the next hop for routes sent to an EBGP peer or a peer group, but not for routes sent to an IBGP peer or a peer group.

Configuring the AS_PATH attribute

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Allow the local AS number to appear in the as-path of routes from a peer or a peer group and specify the number of times that the local AS number can appear in the as-path of routes from the peer or the peer group.	peer { <i>ipv6-group-name</i> <i>ipv6-address</i> } allow-as-loop [<i>number</i>]	Optional. Not allowed by default.
5. Disable IPv6 MBGP from considering the AS_PATH during best route selection.	bestroute as-path-neglect	Optional. Enabled by default.
6. Configure updates to a peer or a peer group to carry only the public AS number.	peer { <i>ipv6-group-name</i> <i>ipv6-address</i> } public-as-only	Optional. By default, outbound IPv6 MBGP updates can carry private AS numbers.

Tuning and optimizing IPv6 MBGP networks

Configuration prerequisites

Before you tune and optimize an OSPF network, complete the following tasks:

- Enable IPv6.
- Configure basic IPv6 MBGP functions.

Configuring IPv6 MBGP soft reset

After you modify a route selection policy, you must reset IPv6 MBGP connections to make the new one take effect.

The current IPv6 MBGP implementation supports the route-refresh feature that enables dynamic route refresh without terminating IPv6 MBGP connections.

If a peer that does not support route refresh exists in the network, you must configure the **peer keep-all-routes** command to save all routes from the peer. When the routing policy is changed, the system will update the IPv6 MBGP routing table and apply the new policy.

Performing soft reset through route refresh

If the peer is enabled with route refresh, when the IPv6 MBGP route selection policy is modified on a router, the router advertises a route-refresh message to its IPv6 MBGP peers, which resend their routing information to the router after they receive the message. Therefore, the local router can perform dynamic route update and apply the new policy without terminating IPv6 MBGP connections.

To configure IPv6 MBGP soft reset through route refresh:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp as-number	N/A
3. Enter IPv6 address family view.	ipv6-family	N/A
4. Enable IPv6 BGP route refresh for a peer or a peer group.	peer { ipv6-group-name ipv6-address } capability-advertise route-refresh	Optional. Enabled by default.

Performing soft reset manually

If the peer does not support route refresh, you can use the **peer keep-all-routes** command to save all the route updates from the peer, and then use the **refresh bgp ipv6 multicast** command to soft-reset IPv6 MBGP connections to refresh the IPv6 MBGP routing table and apply the new policy without terminating IPv6 MBGP connections.

To perform soft reset manually:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp as-number	N/A
3. Enter IPv6 address family view.	ipv6-family	N/A
4. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A

Step	Command	Remarks
5. Keep all routes from a peer or a peer group regardless of whether they pass the inbound filtering policy.	peer { <i>ipv6-group-name</i> <i>ipv6-address</i> } keep-all-routes	Not kept by default.
6. Perform soft reset manually.	refresh bgp ipv6 multicast { all <i>ipv6-address</i> group <i>ipv6-group-name</i> external internal } { export import }	Optional.

Enabling the IPv6 MBGP orf capability

The BGP Outbound Route Filter (ORF) feature enables a BGP speaker to send a set of ORFs to its BGP peer through route-refresh messages. The peer then applies the ORFs, in addition to its local routing policies (if any), to filter updates to the BGP speaker, thus reducing the number of exchanged update messages and saving network resources.

After you enable the ORF capability, the local BGP router negotiates the ORF capability with the BGP peer through open messages. That is, the router determines whether to carry ORF information in messages, and if yes, whether to carry non-standard ORF information in the packets. After completing the negotiation process and establishing the neighboring relationship, the BGP router and its BGP peer can exchange ORF information through specific route-refresh messages.

For the parameters configured on both sides for ORF capability negotiation, see [Table 12](#).

To enable the IPv6 MBGP ORF capability:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv6 address family view.	ipv6-family	N/A
4. Enable BGP route refresh for a peer or a peer group.	peer { <i>group-name</i> <i>ipv6-address</i> } capability-advertise route-refresh	Optional. Enabled by default. If this feature is not enabled, you must configure this command.
5. Enable the non-standard ORF capability for a BGP peer or a peer group.	peer { <i>group-name</i> <i>ipv6-address</i> } capability-advertise orf non-standard	Optional. By default, standard BGP ORF capability defined in RFC 5291 and RFC 5292 is supported. If this feature is not enabled, you must configure this command.
6. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
7. Enable the ORF IP prefix negotiation capability for a BGP peer or a peer group.	peer { <i>group-name</i> <i>ipv6-address</i> } capability-advertise orf ip-prefix { both receive send }	Not enabled by default.

Table 12 Description of the send, receive, and both parameters and the negotiation result

Local parameter	Peer parameter	Negotiation result
send	<ul style="list-style-type: none"> • receive • both 	The ORF sending capability is enabled locally and the ORF receiving capability is enabled on the peer.
receive	<ul style="list-style-type: none"> • send • both 	The ORF receiving capability is enabled locally and the ORF sending capability is enabled on the peer.
both	both	Both the ORF sending and receiving capabilities are enabled locally and on the peer, respectively.

Configuring the maximum number of equal-cost routes for load-balancing

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp as-number	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Configure the maximum number of equal-cost routes for load balancing.	balance number	By default, load balancing is disabled.

Configuring a large scale IPv6 MBGP network

Before you configure the following tasks, you must configure basic IPv6 MBGP functions.

Configuring an IPv6 MBGP peer group

For easy management and configuration, you can organize some IPv6 MBGP peers that have the same route update policy into a peer group. A policy configured for a peer group applies to all the members in the group.

To create an IPv6 MBGP peer group, you must enable an existing IPv6 unicast peer group in IPv6 MBGP address family view.

Before adding an IPv6 MBGP peer to the IPv6 MBGP peer group, you must add the corresponding IPv6 BGP unicast peer to the corresponding IPv6 BGP unicast peer group.

To configure an IPv6 MBGP peer group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv6 address family view.	ipv6-family	N/A
4. Create an IPv6 BGP peer group.	group <i>ipv6-group-name</i> [external internal]	N/A
5. Add a peer to the peer group.	peer <i>ipv6-address</i> group <i>ipv6-group-name</i> [as-number <i>as-number</i>]	By default, no peer is added.
6. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
7. Enable the configured IPv6 unicast BGP peer group to create the IPv6 MBGP peer group.	peer <i>ipv6-group-name</i> enable	N/A
8. Add the IPv6 MBGP peer into the peer group.	peer <i>ipv6-address</i> group <i>ipv6-group-name</i>	By default, no peer is added.

Configuring IPv6 MBGP community

A peer group enables a group of peers to share the same policy, and a community enables a group of IPv6 MBGP routers in multiple ASs to share the same policy. The COMMUNITY attribute is propagated among IPv6 MBGP peers and not restricted to AS boundaries.

You can reference a routing policy to modify the COMMUNITY attribute for routes sent to a peer. In addition, you can define extended community attributes as required.

For more information about routing policy configuration, see *Layer 3—IP Routing Configuration Guide*.

To advertise the COMMUNITY attribute to an IPv6 MBGP peer or a peer group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp <i>as-number</i>	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Advertise the COMMUNITY attribute to an IPv6 MBGP peer or a peer group.	peer { <i>ipv6-group-name</i> <i>ipv6-address</i> } advertise-community	By default, no COMMUNITY attribute is advertised to any peer group/peer.
5. Advertise the extended community attribute to an IPv6 MBGP peer or a peer group.	peer { <i>ipv6-group-name</i> <i>ipv6-address</i> } advertise-ext-community	By default, no extended community attribute is advertised to any peer or peer group.
6. Apply a routing policy to routes sent to an IPv6 MBGP peer or a peer group.	peer { <i>ipv6-group-name</i> <i>ipv6-address</i> } route-policy <i>route-policy-name</i> export	Not configured by default.

NOTE:

You must configure a routing policy to define the **COMMUNITY** attribute, and apply the policy to outgoing routes.

Configuring an IPv6 MBGP route reflector

To guarantee connectivity between IPv6 multicast IBGP peers, you must make them fully meshed. However, this becomes unpractical when too many IPv6 multicast IBGP peers exist. Using route reflectors can solve the problem.

The clients of a route reflector should not be fully meshed, and the route reflector reflects the routes of a client to the other clients. If the clients are fully meshed, you must disable route reflection between clients to reduce routing costs.

If a cluster has multiple route reflectors, you must specify the same cluster ID for these route reflectors to avoid routing loops.

To configure an IPv6 BGP route reflector:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter BGP view.	bgp as-number	N/A
3. Enter IPv6 MBGP address family view.	ipv6-family multicast	N/A
4. Configure the router as a route reflector and specify an IPv6 MBGP peer or a peer group as its client.	peer { ipv6-group-name ipv6-address } reflect-client	Not configured by default.
5. Enable route reflection between clients.	reflect between-clients	Optional. Enabled by default.
6. Configure the cluster ID of the route reflector.	reflector cluster-id cluster-id	Optional. By default, a route reflector uses its router ID as the cluster ID.

Displaying and maintaining IPv6 MBGP

Displaying IPv6 MBGP

Task	Command	Remarks
Display IPv6 MBGP peer group information.	display bgp ipv6 multicast group [<i>ipv6-group-name</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv6 MBGP routing information injected with the network command.	display bgp ipv6 multicast network [{ begin exclude include } <i>regular-expression</i>]	Available in any view

Task	Command	Remarks
Display the IPv6 MBGP AS path information of routes.	display bgp ipv6 multicast paths [<i>as-regular-expression</i> { begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv6 MBGP peer information or peer group information.	display bgp ipv6 multicast peer [[<i>ipv6-address</i>] verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the prefix entries in the ORF information of the specified BGP peer.	display bgp ipv6 multicast peer <i>ipv6-address</i> received ipv6-prefix [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv6 MBGP routing table information.	display bgp ipv6 multicast routing-table [<i>ipv6-address</i> <i>prefix-length</i>] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv6 MBGP routing information that matches an AS path list.	display bgp ipv6 multicast routing-table as-path-acl <i>as-path-acl-number</i> [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv6 MBGP routing information with the specified COMMUNITY attribute.	display bgp ipv6 multicast routing-table community [<i>aa:nn<1-13></i>] [no-advertise no-export no-export-subconfed]* [whole-match] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display routing information matching an IPv6 MBGP community list.	display bgp ipv6 multicast routing-table community-list { { <i>basic-community-list-number</i> <i>comm-list-name</i> } [whole-match] <i>adv-community-list-number</i> } [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv6 MBGP dampened routing information.	display bgp ipv6 multicast routing-table dampened [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv6 MBGP dampening parameter information.	display bgp ipv6 multicast routing-table dampening parameter [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv6 MBGP routing information originated from different ASs.	display bgp ipv6 multicast routing-table different-origin-as [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv6 MBGP routing flap statistics.	display bgp ipv6 multicast routing-table flap-info [regular-expression <i>as-regular-expression</i> [as-path-acl <i>as-path-acl-number</i> <i>ipv6-address</i> <i>prefix-length</i> [longer-match]] [{ begin exclude include } <i>regular-expression</i>]]	Available in any view
Display the IPv6 MBGP routes received from or advertised to the IPv6 MBGP peer or peer group.	display bgp ipv6 multicast routing-table peer <i>ipv6-address</i> { advertised-routes received-routes } [<i>network-address</i> <i>prefix-length</i> statistic] [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display IPv6 multicast routing information matching an AS regular expression.	display bgp ipv6 multicast routing-table regular-expression <i>as-regular-expression</i>	Available in any view
Display IPv6 MBGP routing statistics.	display bgp ipv6 multicast routing-table statistic [{ begin exclude include } <i>regular-expression</i>]	Available in any view
Display the IPv6 MBGP routing table information.	display ipv6 multicast routing-table [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view

Task	Command	Remarks
Display the multicast routing information of the specified destination address.	display ipv6 multicast routing-table <i>ipv6-address prefix-length</i> [longer-match] [verbose] [{ begin exclude include } <i>regular-expression</i>]	Available in any view

Resetting IPv6 MBGP connections

When you change an IPv6 MBGP routing policy, you can make the new configuration effective by resetting the IPv6 MBGP connections.

Task	Command	Remarks
Reset the specified IPv6 MBGP connections.	reset bgp ipv6 multicast { <i>as-number</i> <i>ipv6-address</i> [flap-info] all group <i>ipv6-group-name</i> external internal }	Available in user view

Clearing IPv6 MBGP information

Task	Command	Remarks
Clear dampened IPv6 MBGP routing information and release suppressed routes.	reset bgp ipv6 multicast dampening [<i>ipv6-address prefix-length</i>]	Available in user view
Clear IPv6 MBGP route flap statistics.	reset bgp ipv6 multicast flap-info [<i>ipv6-address/prefix-length</i> regexp <i>as-path-regexp</i> as-path-acl <i>as-path-acl-number</i>]	Available in user view

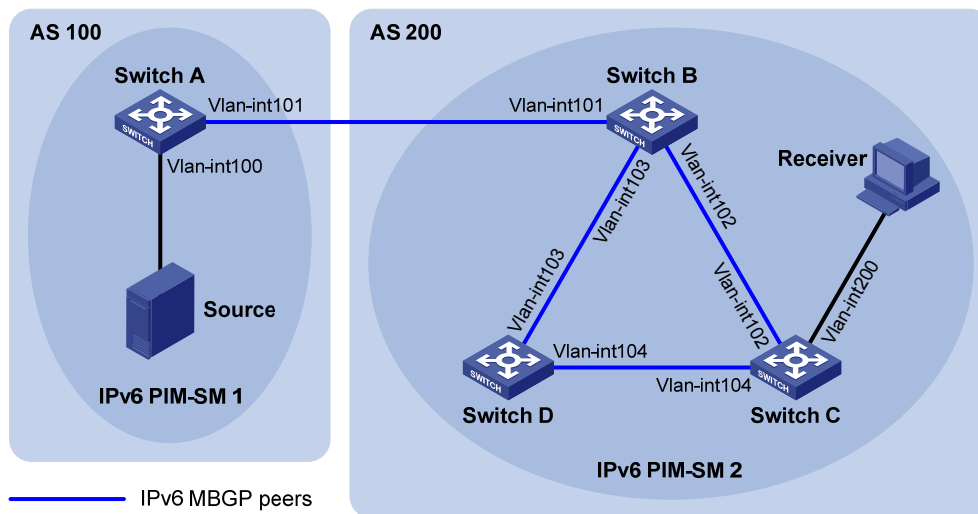
IPv6 MBGP configuration example

Network requirements

As shown in the following figure:

- IPv6 PIM-SM 1 is in AS 100, and IPv6 PIM-SM 2 is in AS 200. OSPFv3 is the IGP in the two ASs, and IPv6 MBGP runs between the two ASs to exchange IPv6 multicast route information.
- The IPv6 multicast source belongs to IPv6 PIM-SM 1 and the receiver belongs to IPv6 PIM-SM 2.
- The VLAN-interface 101 of Switch A and Switch B must be configured as the C-BSR and C-RP of the IPv6 PIM-SM domains.
- Enable the imbedded RP function for all switches in IPv6 PIM domain.

Figure 110 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Source	N/A	1002::100/64	Switch C	Vlan-int200	3002::1/64
Switch A	Vlan-int100	1002::1/64	Switch C	Vlan-int102	2001::2/64
	Vlan-int101	1001::1/64		Vlan-int104	3001::1/64
Switch B	Vlan-int101	1001::2/64	Switch D	Vlan-int103	2002::2/64
	Vlan-int102	2001::1/64		Vlan-int104	3001::2/64
	Vlan-int103	2002::1/64			

Configuration procedure

1. Enable IPv6 and configure IPv6 addresses for interfaces. (Details not shown.)
2. Configure OSPFv3. (Details not shown.)
3. Enable IPv6 multicast routing, IPv6 PIM-SM and MLD, and configure an IPv6 PIM-SM domain border:

Enable IPv6 multicast routing on Switch A, and enable IPv6 PIM-SM on each interface.

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
```

The configuration on Switch B and Switch D is similar to the configuration on Switch A.

Enable IPv6 multicast routing on Switch C, enable IPv6 PIM-SM on each interface, and enable MLD on the host-side interface VLAN-interface 200.

```
<SwitchC> system-view
[SwitchC] multicast ipv6 routing-enable
[SwitchC] interface vlan-interface 102
[SwitchC-Vlan-interface102] pim ipv6 sm
```



```
[SwitchC-Vlan-interface102] quit
[SwitchC] interface vlan-interface 104
[SwitchC-Vlan-interface104] pim ipv6 sm
[SwitchC-Vlan-interface104] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] pim ipv6 sm
[SwitchC-Vlan-interface200] mld enable
[SwitchC-Vlan-interface200] quit
```

Configure an IPv6 PIM domain border on Switch A.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 bsr-boundary
[SwitchA-Vlan-interface101] quit
```

Configure an IPv6 PIM domain border on Switch B.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim ipv6 bsr-boundary
[SwitchB-Vlan-interface101] quit
```

4. Enable the imbedded RP function:

Enable the imbedded RP function on Switch A.

```
[SwitchA] pim ipv6
[SwitchA-pim6] embedded-rp
[SwitchA-pim6] quit
```

Configure Switch B, Switch C, and Switch D in the same way. (Details not shown.)

5. Configure BGP, specify the IPv6 MBGP peer and enable direct route redistribution:

On Switch A, configure the IPv6 MBGP peer and enable direct route redistribution.

```
[SwitchA] bgp 100
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] ipv6-family
[SwitchA-bgp-af-ipv6] peer 1001::2 as-number 200
[SwitchA-bgp-af-ipv6] import-route direct
[SwitchA-bgp-af-ipv6] quit
[SwitchA-bgp] ipv6-family multicast
[SwitchA-bgp-af-ipv6-mul] peer 1001::2 enable
[SwitchA-bgp-af-ipv6-mul] import-route direct
[SwitchA-bgp-af-ipv6-mul] quit
[SwitchA-bgp] quit
```

On Switch B, configure the IPv6 MBGP peers and redistribute OSPF routes.

```
[SwitchB] bgp 200
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] ipv6-family
[SwitchB-bgp-af-ipv6] peer 1001::1 as-number 100
[SwitchB-bgp-af-ipv6] import-route ospfv3 1
[SwitchB-bgp-af-ipv6] quit
[SwitchB-bgp] ipv6-family multicast
[SwitchB-bgp-af-ipv6-mul] peer 1001::1 enable
[SwitchB-bgp-af-ipv6-mul] import-route ospfv3 1
```

```
[SwitchB-bgp-af-ipv6-mul] quit
[SwitchB-bgp] quit
```

6. Verify the configuration:

Use the **display bgp ipv6 multicast peer** command to display IPv6 MBGP peers on a switch. For example:

Display IPv6 MBGP peers on Switch B.

```
[SwitchB] display bgp ipv6 multicast peer
```

```
BGP local router ID : 2.2.2.2
```

```
Local AS number : 200
```

```
Total number of peers : 3
```

```
Peers in established state : 3
```

Peer	AS	MsgRcvd	MsgSent	OutQ	PrefRcv	Up/Down	State
1001::1	100	56	56	0	0	00:40:54	Established

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

<http://www.hp.com/support>

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

<http://www.hp.com/go/wwalerts>

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

<http://www.hp.com/support/manuals>

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Websites

- HP.com <http://www.hp.com>

- HP Networking <http://www.hp.com/go/networking>
- HP manuals <http://www.hp.com/support/manuals>
- HP download drivers and software <http://www.hp.com/support/downloads>
- HP software depot <http://www.software.hp.com>
- HP Education <http://www.hp.com/learn>

Conventions

This section describes the conventions used in this documentation set.




Command conventions


Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> text represents arguments that you replace with actual values.
[]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x y ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x y ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x y ... } *	Asterisk-marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x y ...] *	Asterisk-marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions








Convention	Description
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the New User window appears; click OK .
>	Multi-level menus are separated by angle brackets. For example, File > Create > Folder .

Symbols

Convention	Description
 WARNING	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 CAUTION	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 IMPORTANT	An alert that calls attention to essential information.

Convention	Description
NOTE	An alert that contains additional or supplementary information.
 TIP	An alert that provides helpful information.

Network topology icons

	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the switching engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a security product, such as a firewall, a UTM, or a load-balancing or security card that is installed in a device.
	Represents a security card, such as a firewall card, a load-balancing card, or a NetStream card.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index

A C D E I M O P R T

A

Adjusting IGMP performance, [112](#)

Adjusting MLD performance, [348](#)

Appendix, [306](#)

Appendix, [56](#)

C

Configuration examples, [91](#)

Configuration task list, [85](#)

Configuration task list, [331](#)

Configuring a large scale IPv6 MBGP network, [461](#)

Configuring a large scale MBGP network, [257](#)

Configuring a port-based IPv6 multicast VLAN, [318](#)

Configuring a port-based multicast VLAN, [68](#)

Configuring a sub-VLAN-based IPv6 multicast VLAN, [317](#)

Configuring a sub-VLAN-based multicast VLAN, [67](#)

Configuring an IGMP snooping policy, [32](#)

Configuring an MLD snooping policy, [282](#)

Configuring an MSDP peer connection, [220](#)

Configuring basic IGMP functions, [109](#)

Configuring basic IGMP snooping functions, [22](#)

Configuring basic IPv6 MBGP functions, [451](#)

Configuring basic MBGP functions, [246](#)

Configuring basic MLD functions, [345](#)

Configuring basic MLD snooping functions, [272](#)

Configuring basic MSDP functions, [218](#)

Configuring BIDIR-PIM, [164](#)

Configuring IGMP proxying, [119](#)

Configuring IGMP snooping port functions, [24](#)

Configuring IGMP snooping proxying, [31](#)

Configuring IGMP snooping querier, [29](#)

Configuring IGMP SSM mapping, [118](#)

Configuring IPv6 BIDIR-PIM, [399](#)

Configuring IPv6 MBGP route attributes, [456](#)

Configuring IPv6 multicast routing and forwarding, [331](#)

Configuring IPv6 PIM common features, [410](#)

Configuring IPv6 PIM snooping, [309](#)

Configuring IPv6 PIM-DM, [385](#)

Configuring IPv6 PIM-SM, [388](#)

Configuring IPv6 PIM-SSM, [408](#)

Configuring MBGP route attributes, [252](#)

Configuring MLD proxying, [354](#)

Configuring MLD snooping port functions, [274](#)

Configuring MLD snooping proxying, [281](#)

Configuring MLD snooping querier, [278](#)

Configuring MLD SSM mapping, [353](#)

Configuring multicast routing and forwarding, [86](#)

Configuring PIM common features, [176](#)

Configuring PIM snooping, [59](#)

Configuring PIM-DM, [149](#)

Configuring PIM-SM, [152](#)

Configuring PIM-SSM, [174](#)

Configuring SA messages related parameters, [222](#)

Contacting HP, [469](#)

Controlling route advertisement and reception, [247](#)

Controlling route distribution and reception, [452](#)

Conventions, [470](#)

D

Displaying and maintaining IGMP, [120](#)

Displaying and maintaining IGMP snooping, [39](#)

Displaying and maintaining IPv6 MBGP, [463](#)

Displaying and maintaining IPv6 multicast routing and forwarding, [333](#)

Displaying and maintaining IPv6 multicast VLAN, [320](#)

Displaying and maintaining IPv6 PIM, [417](#)

Displaying and maintaining IPv6 PIM snooping, [310](#)

Displaying and maintaining MBGP, [260](#)

Displaying and maintaining MLD, [356](#)

Displaying and maintaining MLD snooping, [289](#)

Displaying and maintaining MSDP, [225](#)

Displaying and maintaining multicast routing and forwarding, [89](#)

Displaying and maintaining multicast VLAN, [70](#)

Displaying and maintaining PIM, [183](#)

Displaying and maintaining PIM snooping, [60](#)

E

Enabling IP multicast routing, [85](#)

Enabling IPv6 multicast routing, [331](#)

I

IGMP configuration examples, [122](#)

IGMP configuration task list, [108](#)

IGMP snooping configuration examples, [40](#)

IGMP snooping configuration task list, [21](#)

Introduction to multicast, [1](#)

IPv6 MBGP configuration example, [465](#)

IPv6 MBGP configuration task list, [450](#)

IPv6 MBGP overview, [450](#)

IPv6 multicast VLAN configuration examples, [320](#)

IPv6 multicast VLAN configuration task list, [317](#)

IPv6 PIM configuration examples, [418](#)

IPv6 PIM snooping configuration example, [310](#)

M

MBGP configuration example, [261](#)

MBGP configuration task list, [245](#)

MBGP overview, [245](#)

MLD configuration examples, [358](#)

MLD configuration task list, [344](#)

MLD snooping configuration examples, [290](#)

MLD snooping configuration task list, [271](#)

MSDP configuration examples, [226](#)

MSDP configuration task list, [217](#)

Multicast architecture, [7](#)

Multicast models, [6](#)

Multicast packet forwarding mechanism, [13](#)

Multicast support for VPNs, [13](#)

Multicast VLAN configuration examples, [70](#)

Multicast VLAN configuration task list, [67](#)

O

Overview, [315](#)

Overview, [308](#)

Overview, [328](#)

Overview, [366](#)

Overview, [16](#)

Overview, [211](#)

Overview, [101](#)

Overview, [336](#)

Overview, [266](#)

Overview, [65](#)

Overview, [58](#)

Overview, [78](#)

P

PIM configuration examples, [185](#)

PIM overview, [131](#)

PIM snooping configuration example, [60](#)

Protocols and standards, [245](#)

R

Related information, [469](#)

T

Troubleshooting IGMP, [129](#)

Troubleshooting IGMP snooping, [55](#)

Troubleshooting IPv6 multicast policy configuration, [335](#)

Troubleshooting IPv6 PIM configuration, [447](#)

Troubleshooting IPv6 PIM snooping, [313](#)

Troubleshooting MLD, [364](#)

Troubleshooting MLD snooping, [305](#)

Troubleshooting MSDP, [243](#)

Troubleshooting multicast routing and forwarding, [99](#)

Troubleshooting PIM, [208](#)

Troubleshooting PIM snooping, [63](#)

Tuning and optimizing IPv6 MBGP networks, [458](#)

Tuning and optimizing MBGP networks, [254](#)