HP A5820X & A5800 Switch Series
IP Multicast

Configuration Guide

Abstract

This document describes the software features for the HP A Series products and guides you through the software configuration procedures. These configuration guides also provide configuration examples to help you apply software features to different network scenarios.

This documentation is intended for network planners, field technical support and servicing engineers, and network administrators working with the HP A Series products.

Part number: 5998-1624
Software version: : Release 1211
Document version: 5W100-20110430

Legal and notice information

Contents

Configuring IP multicast

This document focuses on the IP multicast technology and device operations. Unless otherwise stated, the term *multicast* in this document refers to IP multicast.

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.

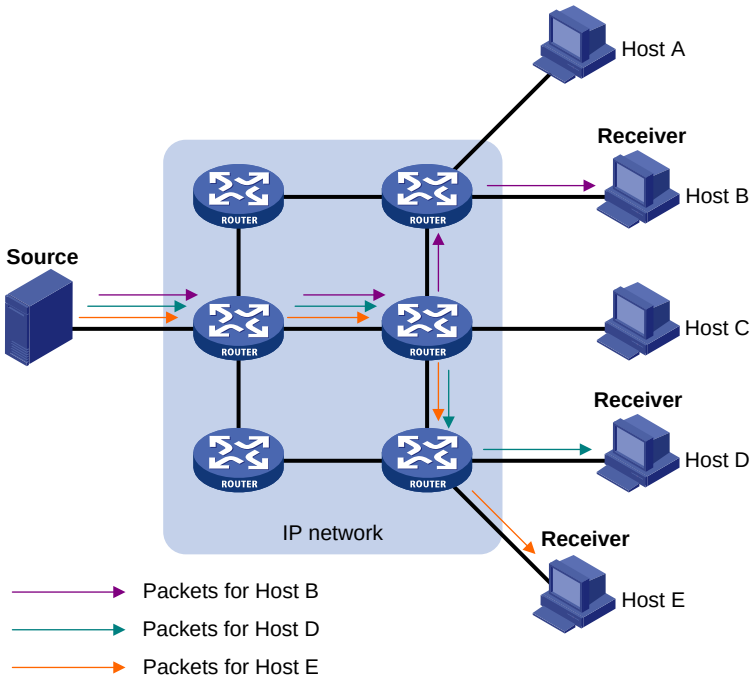
Comparing information transmission techniques

As an information transmission 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.

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 Hosts B, D, and 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 users need the information, the information source must send a

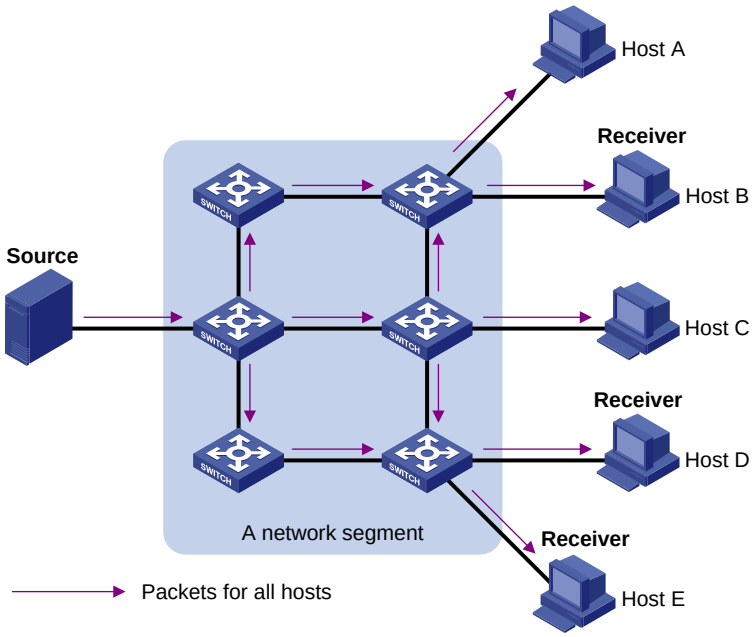
copy of the same information to each of these users. Sending many copies can place tremendous pressure on the information source and the network bandwidth.

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



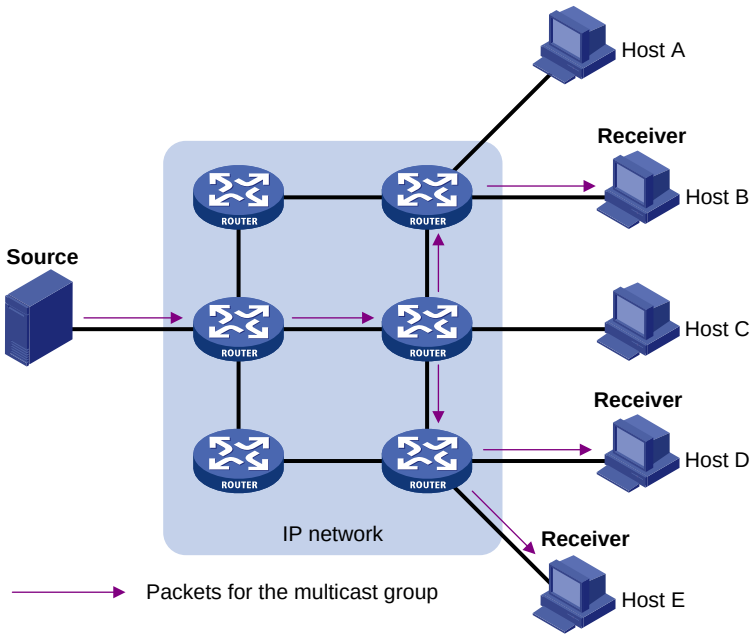
In Figure 2, assume that only Hosts B, D, and E need the information. If the information is broadcast to the subnet, Hosts A and C also receive it. In addition to information security issues, broadcasting to hosts that do not need the information causes traffic flooding on the same subnet.

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. In Figure 3, Hosts B, D, and 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 Hosts B, D, and E.

The advantages of multicast over unicast and broadcast include:

- **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 and does not significatly add to the usage of network resources.
- **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, while multicast is not.

Multicast features

Multicast features include:

- 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

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 with the transmission of TV programs.

Table 1 An analogy between TV 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.

Multicast common notations

The following notations are commonly used in multicast transmission:

- **(*, G)**—An RPT or a multicast packet that any multicast source sends to multicast group G. The asterisk represents any multicast source and the G represents a specific multicast group.
- **(S, G)**—An SPT or a multicast packet that multicast source S sends to multicast group G. The S represents a specific multicast source and the G represents a specific multicast group.

For more information about the concepts of rendezvous point tree and shortest path tree, see *IP Multicast Configuration Guide*.

Multicast advantages and applications

Advantages of multicast include:

- **Enhanced efficiency**—Reduces the processor load related to information source servers and network devices.
- **Optimal performance**—Reduces redundant traffic.
- **Distributed application**—Enables point-to-multipoint applications using minimul network resources.

Applications of multicast include:

- Multimedia and streaming applications, such as web TV, web radio, and realtime 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

Multicast models, including ASM, SFM, and SSM, determine how receivers treat multicast sources.

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 determine the position of 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. In the SFM 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, not all multicast sources are valid because they are filtered.

SSM model

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

The primary 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 is an end-to-end service with architecture that involves several key areas, including:

- **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) enable 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.

IPv4 multicast addresses

IANA assigned the Class D address space (224.0.0.0 to 239.255.255.255) for 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 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: • 232.0.0.0/8—SSM group addresses • 233.0.0.0/8—Glop group addresses
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.

Group membership is dynamic (hosts can join or leave multicast groups at any time).

Glop is a mechanism for assigning multicast addresses between different ASs. For example, filling an AS number into the middle two bytes of 233.0.0.0 provides 255 multicast addresses for that AS. For more information, see RFC 2770.

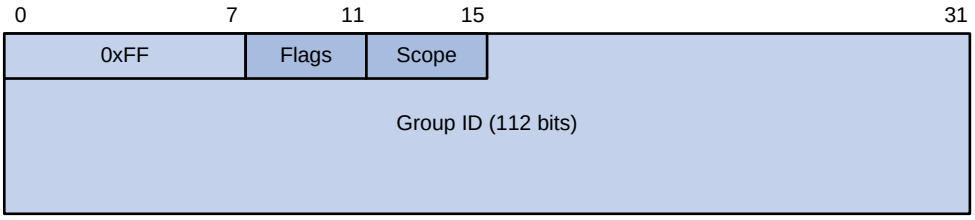
Table 3 Table Some reserved multicast addresses

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	DVMRP routers
224.0.0.5	OSPF routers
224.0.0.6	OSPF designated routers and backup designated routers
224.0.0.7	ST routers
224.0.0.8	ST hosts
224.0.0.9	RIPv2 routers
224.0.0.11	Mobile agents

Address	Description
224.0.0.12	DHCP server/relay agent
224.0.0.13	All PIM routers
224.0.0.14	RSVP encapsulation
224.0.0.15	All CBT routers
224.0.0.16	Designated SBM
224.0.0.17	All SBMs
224.0.0.18	VRRP

IPv6 multicast addresses

Figure 4 IPv6 multicast format



Referring to Figure 4, the fields of an IPv6 multicast address indicate the following:

- **0xFF**—Most significant eight bits are 11111111, indicating that this address is an IPv6 multicast address.
- **Flags**—Contains four bits.

Figure 5 Format of the Flags field

Table 4 Description of the Flags field bits

Bit	Description
0	Reserved, set to 0.
R	• 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	• 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	• 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**—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**—Contains 112 bits and uniquely identifies an IPv6 multicast group that is within the scope defined by the Scope field.

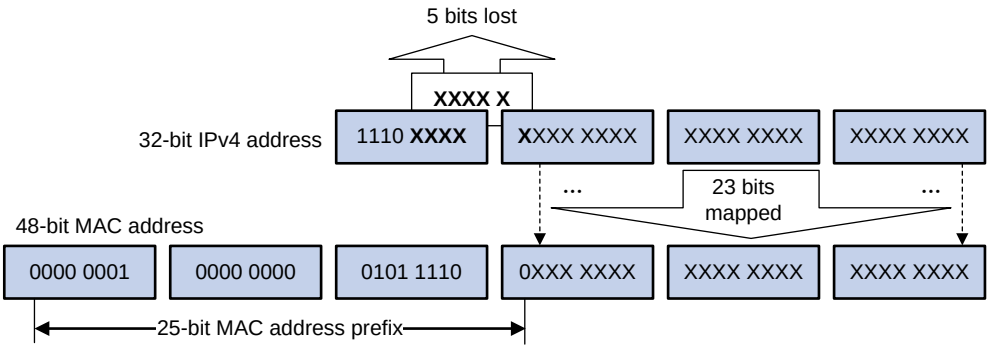
Ethernet multicast MAC addresses

When a unicast IP packet is transmitted over Ethernet, the destination MAC address is the MAC address of the receiver. When a multicast packet is transmitted over Ethernet, the destination address is a multicast MAC address because the packet is directed to a group formed by a number of receivers, rather than to one specific receiver.

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 remaining 23 bits are the least-significant 23 bits of a multicast IPv4 address.

Figure 6 IPv4-to-MAC address mapping

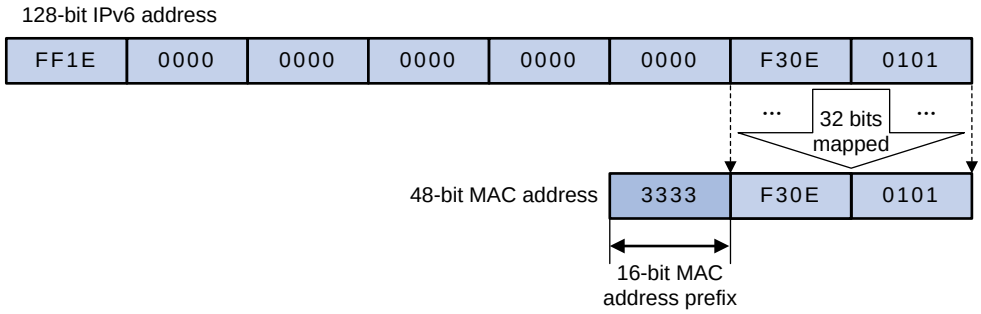


The most-significant four bits of a multicast IPv4 address are 1110, which indicates that this address is a multicast address. Only 23 bits of the remaining 28 bits are mapped to a MAC address, so five bits of the multicast IPv4 address are lost. As a result, 32 multicast IPv4 addresses map to the same IPv4 multicast MAC address. Therefore, in Layer 2 multicast forwarding, a device 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 remaining 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, and MBGP/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, and multicast VLAN/IPv6 multicast VLAN.

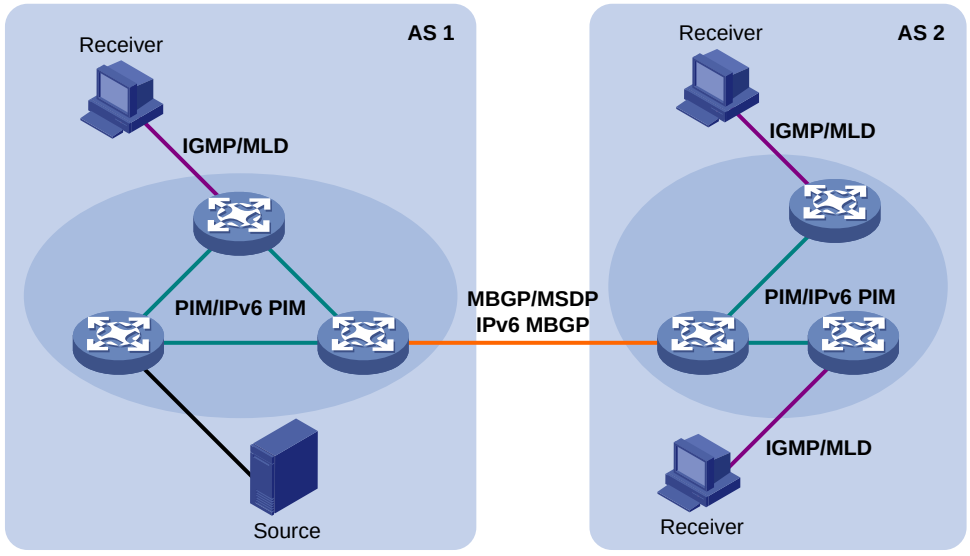
IGMP snooping, IGMP, multicast VLAN, PIM, MSDP, and MBGP are for IPv4. MLD snooping, MLD, IPv6 multicast VLAN, IPv6 PIM, and IPv6 MBGP are for IPv6.

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 documents in the *IP* Multicast *Configuration Guide*.

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, IGMP or MLD is used between hosts and Layer 3 multicast devices directly connected 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 to forward multicast packets correctly and efficiently. Multicast routes are loop-free data transmission paths from a data source to multiple receivers (a multicast distribution tree).

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

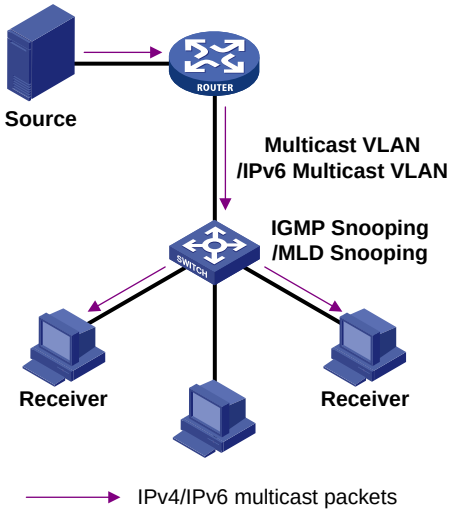
- An intra-domain multicast routing protocol discovers multicast sources and builds multicast distribution trees within an AS to deliver multicast data to receivers. Among a variety of mature intra-domain multicast routing protocols, PIM is most widely used. Based on the forwarding mechanism, PIM has **dense** mode, often called PIM-DM, and **sparse** mode, often called PIM-SM.
- An inter-domain multicast routing protocol delivers multicast information between two ASs. Mature solutions include MSDP and MBGP. MSDP propagates multicast source information among different ASs and MBGP is an extension of 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 positions of the multicast sources, 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 and multicast VLAN/IPv6 multicast VLAN.

Figure 9 Positions of Layer 2 multicast protocols



IGMP snooping/MLD snooping

IGMP snooping and MLD snooping are multicast constraining mechanisms that run on Layer 2 devices. They manage and control multicast groups by listening to 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.

Multicast VLAN/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 needs to 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 the multicast data 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 in different parts of the network, multicast routers on the forwarding path usually need to forward multicast packets received on one incoming interface to multiple outgoing interfaces.

Compared with a unicast model, a multicast model is more complex in the following aspects:

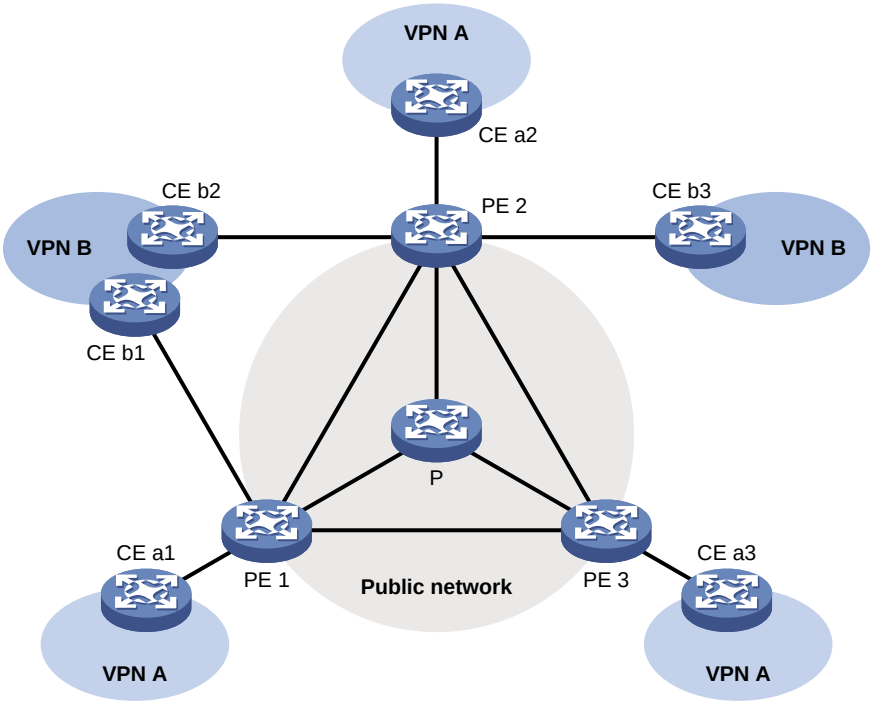
- To ensure multicast packet transmission in the network, unicast routing tables or multicast routing tables (for example, MBGP routing table) specially provided for multicast must be used as guidance for multicast forwarding.
- To process the same multicast information from different peers received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

For more information about the RPF mechanism, see the *IP Multicast Configuration Guide*.

Multi-instance multicast

Multi-instance multicast refers to multicast in a VPN. VPN networks must be isolated from one another and from the public network.

Figure 10 Networking diagram for VPN



As shown in Figure 10, VPN A and VPN B separately access the public network through PE devices. The devices in the network are as follows:

- P device belongs to the public network. The CE devices belong to their respective VPNs. Each CE device serves its own network and maintains only one set of forwarding mechanisms.
- PE devices connect to the public network and the VPN networks at the same time. Each PE device must strictly distinguish the information for different networks and must maintain a separate forwarding mechanism for each network. On a PE device, a set of software and hardware that serves the same network forms an instance. Multiple instances exist on a PE device at the same time, and an instance resides on different PE devices.

Multi-instance multicast applications

With multi-instance multicast enabled, a PE can do the following:

- Maintain a set of independent multicast forwarding mechanisms for each instance, including various multicast protocols, a list of PIM neighbors, and a multicast routing table per instance. Each instance searches its own forwarding table or routing table to forward multicast data.
- Guarantee the isolation between different VPN instances.
- Implement information exchange and data conversion between the public network and VPN instances.

Multi-instance multicast is the basis of multicast over a VPN network. As shown in Figure 10, when a multicast source in VPN A sends a multicast stream to a multicast group, of all possible receivers on the network for that group, only those that belong to VPN A can receive the multicast stream. The multicast data is multicast both in VPN A and in the public network.

Only one set of unified multicast service runs on a non-PE device. It is called a “public instance.”

The configuration made in VPN instance view takes effect only on the VPN instance interface. An interface that does not belong to any VPN instance is called a "public instance interface."

For more information about multicast VPN, see *IP Multicast Configuration Guide*.

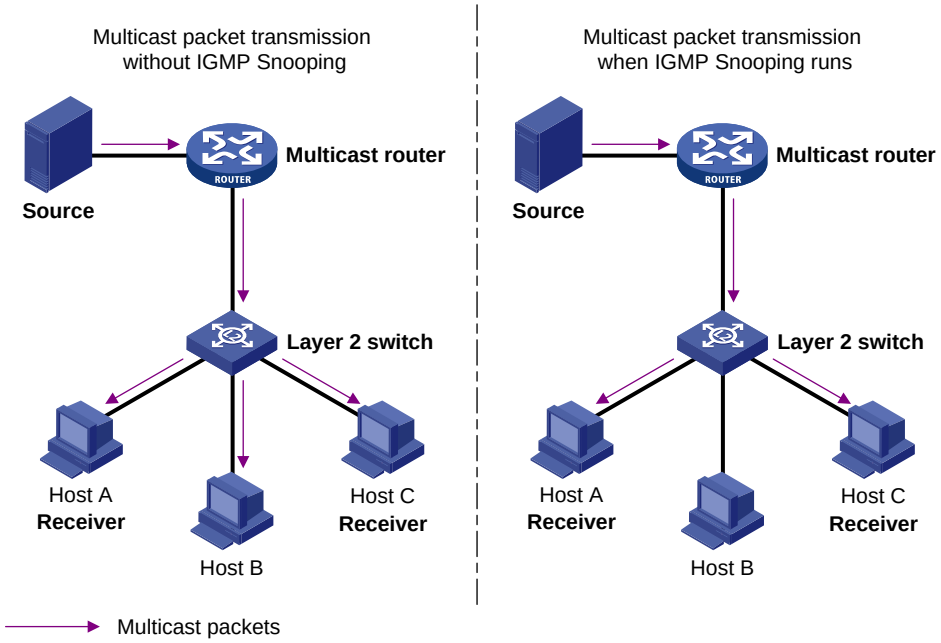
Configuring IGMP snooping

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 switch that is running IGMP snooping establishes mappings between ports and multicast MAC addresses and forwards multicast data based on these mappings.

When IGMP snooping is not running on the switch, multicast packets are broadcast to all devices at Layer 2. When IGMP snooping is running on the switch, multicast packets for known multicast groups are multicast to the receivers, rather than broadcast to all hosts, at Layer 2.

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



IGMP snooping forwards multicast data to the receivers that require the data at Layer 2 only, and provides the following advantages:

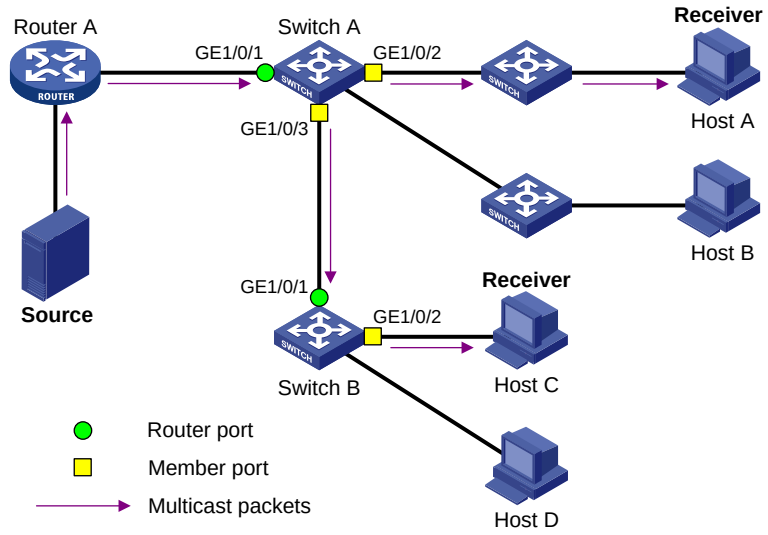
- Reducing Layer 2 broadcast packets, saving network bandwidth.
- Enhancing the security of multicast traffic.
- Facilitating the implementation of per-host accounting.

In this document, a router port is a port on the switch that leads the switch to a Layer 3 multicast device, rather than a port on a router. Unless otherwise specified, router/member ports mentioned include static and dynamic ports.

An IGMP-snooping-enabled switch deems that all ports on which IGMP general queries with the source IP address other than 0.0.0.0 or PIM hello messages are received are dynamic router ports. For more information about PIM hello messages, see "Configuring PIM."

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, also called multicast group members.

Figure 12 IGMP snooping related ports



IGMP snooping involves the following ports:

- **Router port**—A router port is a port on a Layer 2 switch that leads toward a Layer 3 multicast device (DR or IGMP querier). In Figure 12, GigabitEthernet 1/0/1 of Switch A and GigabitEthernet 1/0/1 of Switch B are router ports. Each switch registers all its local router ports in its router port list.
- **Member port**—A member port is a port on a Layer 2 switch that leads toward multicast group members. 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. Each switch registers all the member ports on the local device in its IGMP snooping forwarding table.

Table 6 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 sets a timer initialized to the dynamic router port aging time.	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 sets a timer for the port, which is initialized to the dynamic member port aging time.	IGMP membership report	The switch removes this port from the IGMP snooping forwarding table.

The port aging mechanism of IGMP snooping works only for dynamic ports; a static port will never age out.

IGMP snooping process

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

The description about adding or deleting a port in this section is only for a dynamic port. Static ports can be added or deleted only through the corresponding configurations. For more information, see "Configuring static ports."

Receiving a general query

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

Upon receiving an IGMP general query, the switch forwards it through all ports in the VLAN (except the receiving port) and performs the following on the receiving port:

- If the receiving port is a dynamic router port that exists in its router port list, the switch resets the aging timer for this dynamic router port.
- If the receiving port is not a dynamic router port that exists in its router port list, the switch adds it into its router port list and sets an aging timer for this dynamic router port.

Receiving a membership report

A host sends an IGMP report to the IGMP querier in the following circumstances:

- If the host is already a member of a multicast group, the host responds with an IGMP report after receiving an IGMP query.
- to join a multicast group, the host sends an IGMP report to the IGMP querier to announce that it is interested in the multicast information addressed to that 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, and performs the following operations:

- If no entry in the forwarding table exists for the reported group, the switch creates an entry, adds the port as a dynamic member port to the outgoing port list, and starts a member port aging timer for that port.
- If an entry in the forwarding table exists for the reported group, but the port is not included in the outgoing port list for that group, the switch adds the port as a dynamic member port to the outgoing port list and starts an aging timer for that port.
- If an entry in the forwarding table exists for the reported group and the port is included in the outgoing port list, which means that this port is already a dynamic member port, the switch resets the aging timer for that port.

A switch does not forward an IGMP report through a nonrouter port. This is because if the switch forwards a report message through a member port, all the attached hosts that are monitoring the reported multicast address will suppress their own reports upon receiving this report according to the IGMP report suppression mechanism on them. This will prevent the switch from determining whether the reported multicast group still has active members attached to that port.

For more information about IGMP report suppression mechanism on a host, see the *IP Multicast Configuration Guide*.

Receiving a leave message

When an IGMPv1 host leaves a multicast group, the host does not send an IGMP leave message, so the switch cannot determine immediately that the host has left the multicast group. However, as the host stops sending IGMP reports as soon as it leaves a multicast group, the switch deletes the forwarding entry for the dynamic member port corresponding to the host from the forwarding table when its aging timer 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 determines whether an entry in the forwarding table exists for the group address in the message, and, if one exists, whether the outgoing port list contains the port.

- If the entry in the forwarding table does not exist or if the outgoing port list does not contain the port, the switch discards the IGMP leave message instead of forwarding it to any port.
- If the entry in the forwarding table exists and the outgoing port list contains the port, the switch forwards the leave message to all router ports in the native VLAN. Because the switch cannot determine whether any other hosts attached to the port are still monitoring that group address, the switch does not immediately remove the port from the outgoing port list of the entry in the forwarding table for that group. Instead, it resets the aging timer for the port.

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

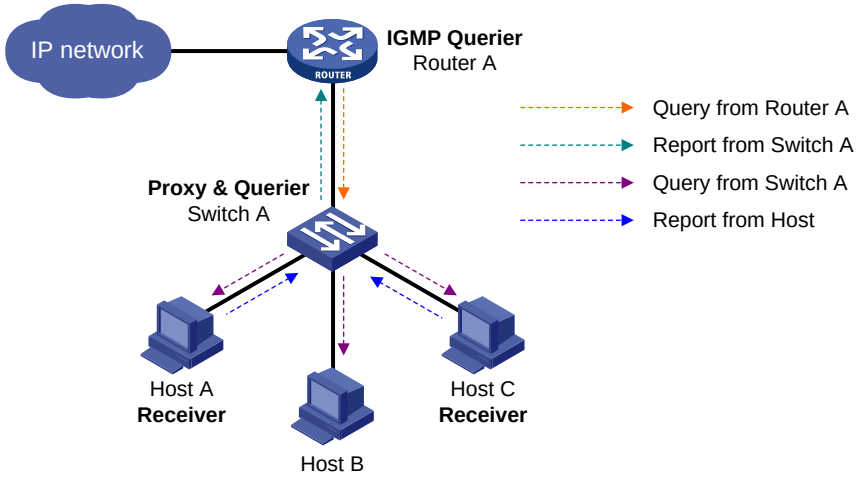
- If any IGMP report in response to the group-specific query is received on the port (suppose it is a dynamic member port) before its aging timer expires, a host attached to the port is receiving or expecting to receive multicast data for that multicast group. The switch resets the aging timer of the port.
- If no IGMP report in response to the group-specific query is received on the port before its aging timer expires, no hosts attached to the port are still monitoring that group address. The switch removes the port from the outgoing port list of the entry in the forwarding table for that multicast group when the aging timer expires.

IGMP snooping proxying

The IGMP snooping proxying function on an edge device reduces the number of IGMP reports and leave messages sent to its upstream device. The device configured with IGMP snooping proxying is a host from the perspective of its upstream device and is referred to as the IGMP snooping proxy.

Although an upstream device considers IGMP snooping proxy a host, the IGMP membership report suppression mechanism for hosts does not take effect. For more information about this mechanism, see *IP Multicast Configuration Guide*.

Figure 13 Figure Network diagram for IGMP snooping proxying



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 7 IGMP message processing on an IGMP snooping proxy

IGMP message	Actions
General query	When receiving an IGMP general query, the proxy forwards the query to all ports except the receiving port. In addition, the proxy generates a report according to the group memberships it maintains and sends the report out all router ports.
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 all router ports if the forwarding entry for the group still contains a member port.
Report	When receiving a report for a multicast group, the proxy looks up the multicast forwarding table for the entry for the multicast group. If the forwarding entry is found with the receiving port contained as a dynamic member port in the outgoing port list, the proxy resets the aging timer for the entry. If the forwarding entry is found but the outgoing port list does not include the receiving port, the proxy adds the port to the outgoing port list as a dynamic member port and starts an aging timer for it. If no forwarding entry is found, the proxy creates the entry, adds the receiving port to the outgoing port list as a dynamic member port and starts an aging timer for the port, and then sends a report to the group out all router ports.
Leave	In response to an IGMP leave message for a multicast group, the proxy sends a group-specific query out 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 all router ports.

IGMP snooping multicast protocol messages

With Layer 3 multicast routing enabled, an IGMP snooping–enabled switch processes multicast protocol messages according to the following conditions:

- Only IGMP is enabled on the switch, or both IGMP and PIM are enabled on the switch, the switch handles multicast protocol messages in the normal way.
- Only PIM is enabled on the switch:
  - The switch broadcasts IGMP messages as unknown messages in the VLAN.
  - Upon receiving a PIM hello message, the switch maintains the corresponding dynamic router port.
- IGMP is disabled on the switch:
  - 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 without deleting its dynamic router ports.
- 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.

On a switch with Layer 3 multicast routing enabled, use **display igmp group port-info** to view Layer 2 port information. For more information about this command, see *IP Multicast Command Reference*.

Protocols and standards

IGMP snooping is documented in RFC 4541—*Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*.

Configuring IGMP snooping basic functions

IGMP snooping requires configuration of the basic functions, and all other configuration tasks are optional.

- Configurations made in IGMP snooping view are effective for all VLANs, while configurations made in VLAN view are effective only for ports belonging to the current VLAN. For a given VLAN, a configuration made in IGMP snooping view is effective only if the same configuration is not made in VLAN view.
- Configurations made in IGMP snooping view are effective for all ports; configurations made in Ethernet interface view are effective only for the current port; configurations made in Layer 2 aggregate interface view are effect only for the current interface; configurations made in port group view are effective only for all the ports in the current port group. For a given port, a configuration made in IGMP snooping view is effective only if the same configuration is not made in Ethernet interface view, Layer 2 aggregate interface view or port group view.
- Configurations made on a Layer 2 aggregate interface do not interfere with configurations made on its member ports, nor do they take part in aggregation calculations; configurations made on a member port of the aggregate group will not take effect until it leaves the aggregate group.

Prerequisites

Before configuring the basic functions of IGMP snooping, complete the following tasks:

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

Enabling IGMP snooping

Enable IGMP snooping globally before enabling it in a VLAN. After enabling IGMP snooping in a VLAN, you cannot enable IGMP or PIM on the corresponding VLAN interface. When you enable IGMP snooping in a specified VLAN, this function takes effect for the ports in this VLAN only.

On an A5800 switch:

- Without MPLS enabled, the switch can have up to 4000 multicast forwarding entries, including IPv4 Layer 2 and Layer 3 multicast forwarding entries, and IPv6 Layer 2 and Layer 3 multicast forwarding entries. If the number of the multicast forwarding entries on the switch is more than 3000, do not configure MPLS on the switch.
- With MPLS enabled, the switch can have up to 3000 multicast forwarding entries.

For more information about MPLS, see *MPLS Configuration Guide*.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enable IGMP snooping globally and enter IGMP snooping view.	**igmp-snooping**	Required. Defaults to disabled.
3. Return to system view.	**quit**	—
4. Enter VLAN view.	**vlan** *vlan-id*	—
5. Enable IGMP snooping in the VLAN.	**igmp-snooping enable**	Required. Defaults to disabled.

Configuring the IGMP snooping version

Configuring an IGMP snooping version includes the version of IGMP messages that IGMP snooping can process.

- IGMP snooping version 2 can process IGMPv1 and IGMPv2 messages, but not IGMPv3 messages, which will be flooded in the VLAN.
- IGMP snooping version 3 can process IGMPv1, IGMPv2, and IGMPv3 messages.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Configure the version of IGMP snooping.	**igmp-snooping version** *version-number*	Optional. Defaults to version 2.

If you switch IGMP snooping from version 3 to version 2, the system takes the following action:

- Clears all IGMP snooping forwarding entries from dynamic joins.

- Keeps forwarding entries for version 3 static (*, G) joins.
- Clears forwarding entries from version 3 static (S, G) joins, which are restored when IGMP snooping is switched back to version 3.

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. You can also configure static multicast MAC address entries.

Configuring a static multicast MAC address entry in system view

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Configure a static multicast MAC address entry.	**mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	Required. No static multicast MAC address entries exist by default.

Configuring a static multicast MAC address entry in interface view

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required Changes made in Ethernet interface view or in Layer 2 aggregate interface view take effect only on the current interface. In port group view, the configuration takes effect on all ports in the port group.
3. Configure a static multicast MAC address entry.	**mac-address multicast** *mac-address* **vlan** *vlan-id*	Required No static multicast MAC address entries exist by default.

When you configure a static multicast MAC address entry in system view, the configuration is effective for the specified interface. When you configure a static multicast MAC address entry in interface view or port group view, the configuration is effective only for the current interface or interfaces in the current port group.

Any legal multicast MAC address except 0100-5Exx-xxxx (with x representing a hexadecimal number from 0 to F) can be manually added to the multicast MAC address table.

Configuring IGMP snooping port functions

Prerequisites

Before configuring 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.

Configuring aging timers for dynamic ports

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

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

If multicast group memberships change frequently, set a relatively small value for the dynamic member port aging timer, and vice versa.

Configuring aging timers for dynamic ports globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IGMP snooping view.	**igmp-snooping**	—
3. Configure dynamic router port aging time.	**router-aging-time** *interval*	Optional. Defaults to105 seconds.
4. Configure dynamic member port aging time.	**host-aging-time** *interval*	Optional Defaults to 260 seconds.

Configuring aging timers for dynamic ports in a VLAN

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Configure dynamic router port aging time.	**igmp-snooping router-aging-time** *interval*	Optional. Defaults to 105 seconds.
4. Configure dynamic member port aging time.	**igmp-snooping host-aging-time** *interval*	Optional. Defaults to 260 seconds.

Configuring static ports

To ensure that all the hosts attached to a port are available for the multicast data addressed to a particular multicast group or the multicast data that a particular multicast source sends to a particular group, configure static (*, G) or (S, G) joining on that port (configure the port as a group-specific or source-and-group-specific static member port).

Configure a port of a switch to be a static router port, through which the switch can forward all the multicast traffic it received.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Configure the port(s) as static member port(s).	**igmp-snooping static-group** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	Required. No static member ports by default.
4. Configure the port(s) as static router port(s).	**igmp-snooping static-router-port vlan** *vlan-id*	Required. No static router ports by default.

A static (S, G) joining can take effect only if a valid multicast source address is specified and IGMP snooping version 3 is currently running.

A static member port does not respond to queries from the IGMP querier. When static (*, G) or (S, G) joining is enabled or disabled on a port, the port does not send an unsolicited IGMP report or an IGMP leave message.

If IGMP is enabled on the virtual interface of a VLAN and you want a port in that VLAN to be a static multicast group or source-group member port, in addition to configuring the port as a static member port, you must use the **igmp static-group** command to configure the VLAN interface to be a static member of the multicast group or source and group. For more information about the **igmp static-group** command, see the *IP Multicast Command Reference*.

Static member ports and static router ports never age out. To remove such a port, use the corresponding **undo** command.

Configuring simulated joining

Generally, a host running IGMP responds to IGMP queries from the IGMP querier. If a host fails to respond, the multicast router can determine that no member of this multicast group exists on the network segment and remove the corresponding forwarding path.

To avoid this issue, enable simulated joining on the switch port (configure the port as a simulated member host for a multicast group). When receiving an IGMP query, the simulated host responds and the switch can continue receiving multicast data.

A simulated host acts like a real host under the following conditions:

- When a port is configured as a simulated member host, the switch sends an unsolicited IGMP report through that port.
- After a port is configured as a simulated member host, the switch responds to IGMP general queries by sending IGMP reports through that port.
- When the simulated joining function is disabled on a port, the switch sends an IGMP leave message through that port.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—

To do...	Use the command...	Remarks
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Configure simulated (*, G) or (S, G) joining.	**igmp-snooping host-join** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	Required. Defaults to disabled.

Each simulated host is equivalent to an independent host. For example, when simulated hosts receive an IGMP query, the simulated host that corresponds to each configuration responds respectively.

Unlike a static member port, a port configured as a simulated member host will age out like a dynamic member port.

Configuring fast leave processing

The fast leave processing feature enables the switch to process IGMP leave messages quickly. With the fast leave processing feature enabled, when the switch receives an IGMP leave message on a port, the switch immediately removes that port from the outgoing port list of the entry in the forwarding table for the indicated group. Then, when the switch receives IGMP group-specific queries for that multicast group, the switch will not forward them to that port.

In VLANs where only one host is attached to each port, fast leave processing helps improve bandwidth and resource usage. However, if fast leave processing is enabled on a port to which more than one host is attached, when one host leaves a multicast group, the other hosts attached to the port and available for the same multicast group fail to receive multicast data for that group. If the function of dropping unknown multicast traffic is already enabled on the switch or in the VLANs, you should not enable fast leave processing.

Configuring fast leave processing globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IGMP snooping view.	**igmp-snooping**	—
3. Enable fast leave processing.	**fast-leave** [**vlan** *vlan-list*]	Required. Defaults to disabled.

Configuring fast leave processing on a port or a group of ports

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Enable fast leave processing.	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	Required. Defaults to disabled.

Disabling a port or a group of ports from changing into dynamic router ports

A multicast access network can have the following issues:

- Upon receiving an IGMP general query or a PIM Hello message from a connected host, a switch port becomes a dynamic router port. Before its timer expires, this dynamic router port receives all multicast packets within the VLAN it belongs to and forwards them to the host. This affects normal multicast reception of the host.
- The IGMP general query or PIM Hello message sent from the host affects the multicast routing protocol state on Layer 3 devices, such as the IGMP querier or DR election, and can cause network interruption.

To resolve these issues and to enhance network security and control over multicast users, disable the switch port from changing into a dynamic router port upon receiving an IGMP general query or a PIM Hello message.

This configuration does not affect the static router port configuration.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Disable the port or group of ports from changing into dynamic router ports.	**igmp-snooping router-port-deny** [**vlan** *vlan-list*]	Required. By default, the port or group of ports can change into dynamic router ports.

Configuring IGMP snooping querier

Prerequisites

Before configuring the 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 time to 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 running IGMP, a multicast router or Layer 3 multicast device sends IGMP general 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 device is called the "IGMP snooping querier."

A Layer 2 multicast switch does not support IGMP and cannot send general queries by default. By enabling IGMP snooping on a Layer 2 switch in a VLAN where multicast traffic must be Layer-2-switched only and no multicast routers are present, the Layer 2 switch acts as the IGMP snooping querier to send IGMP queries. You can then establish and maintain multicast forwarding entries at the data link layer.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Enable IGMP snooping querier.	**igmp-snooping querier**	Required. Defaults to disabled.

It is meaningless to configure an IGMP snooping querier in a multicast network running IGMP. Although an IGMP snooping querier does not participate in IGMP querier elections, it can affect IGMP querier elections because it sends IGMP general queries with a low source IP address.

For more information about the IGMP snooping querier, see *IP Multicast Configuration Guide*.

Configuring IGMP queries and responses

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

Upon receiving an IGMP query (general query or group-specific query), a host starts a timer for each multicast group that it has joined. This timer is initialized to a random value in the range of 0 to the maximum response time (the host obtains the value of the maximum response time from the Max Response Time field in the IGMP query that it received). When the timer value reaches 0, the host sends an IGMP report to the corresponding multicast group.

An appropriate setting for the maximum response time for IGMP queries enables hosts to respond to queries quickly and avoids bursts of IGMP traffic on the network. Such bursts can occur when a large number of hosts simultaneously send reports when the corresponding timers expire simultaneously.

- For IGMP general queries, configure the maximum response time to fill the Max Response time field.
- For IGMP group-specific queries, configure the IGMP last-member query interval to fill the Max Response time field (for IGMP group-specific queries, the maximum response time equals the IGMP last-member query interval).

Configuring IGMP queries and responses globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IGMP snooping view.	**igmp-snooping**	—
3. Configure the maximum response time to IGMP general queries.	**max-response-time** *interval*	Optional. Defaults to 10 seconds.
4. Configure the IGMP last-member query interval.	**last-member-query-interval** *interval*	Optional. Defaults to 1 second.

Configuring IGMP queries and responses in a VLAN

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Configure IGMP general query interval.	**igmp-snooping query-interval** *interval*	Optional. Defaults to 60 seconds.
4. Configure the maximum response time to IGMP general queries.	**igmp-snooping max-response-time** *interval*	Optional. Defaults to 10 seconds.
5. Configure the IGMP last-member query interval.	**igmp-snooping last-member-query-interval** *interval*	Optional. Defaults to 1 second.

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

Configuring source IP address of IGMP queries

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

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Configure the source address of IGMP general queries.	**igmp-snooping general-query source-ip** { *ip-address* | **current-interface** }	Optional. Defaults to 0.0.0.0.
4. Configure the source IP address of IGMP group-specific queries.	**igmp-snooping special-query source-ip** { *ip-address* | **current-interface** }	Optional. Defaults to 0.0.0.0.

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

Configuring IGMP snooping proxying

Prerequisites

Before configuring 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 switch works as the IGMP snooping proxy for the downstream hosts and upstream router in the VLAN.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Enable IGMP snooping proxying in the VLAN.	**igmp-snooping proxying enable**	Required. Defaults to disabled.

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 sent by the IGMP snooping proxy on behalf of its attached hosts.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Configure a source IP address for the IGMP reports sent by the proxy.	**igmp-snooping report source-ip** { *ip-address* | **current-interface** }	Required. Defaults to 0.0.0.0.
4. Configure a source IP address for the IGMP leave messages sent by the proxy.	**igmp-snooping leave source-ip** { *ip-address* | **current-interface** }	Defaults to 0.0.0.0.

Configuring an IGMP snooping policy

Prerequisites

Before configuring an IGMP snooping policy, complete the following tasks:

- Enable IGMP snooping in the VLAN.
- Determine the ACL rules for multicast group filtering.
- Determine the maximum number of multicast groups that can pass the ports.
- Determine the 802.1p precedence for IGMP messages.

Configuring a multicast group filter

On an IGMP snooping–enabled switch, a multicast group filter enables the service provider to define restrictions on multicast programs available to different users.

In an application, when a user requests a multicast program, the user's host initiates an IGMP report. Upon receiving this report message, the switch compares the report to the configured ACL rule. If the port

on which the report was received can join this multicast group, the switch adds an entry for this port in the IGMP snooping forwarding table. Otherwise, the switch drops this report message. Any multicast data that has failed the ACL evaluation is not sent to this port. In this way, the service provider can control the VOD programs provided for multicast users.

Configuring a multicast group filter globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IGMP snooping view.	**igmp-snooping**	—
3. Configure a multicast group filter.	**group-policy** *acl-number* [**vlan** *vlan-list*]	Required. By default, no group filter is globally configured. The hosts in a VLAN can join any valid multicast group.

Configuring a multicast group filter on a port or a group of ports

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Configure a multicast group filter.	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	Required. By default, no group filter is configured on the current port. The hosts on this port can join any valid multicast group.

Configuring multicast source port filtering

With the multicast source port filtering feature enabled on a port, the port can be connected with multicast receivers only, rather than with multicast sources. This occurs 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 be connected with both multicast sources and multicast receivers.

Configuring multicast source port filtering globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IGMP snooping view.	**igmp-snooping**	—
3. Enable multicast source port filtering.	**source-deny port** *interface-list*	Required. Defaults to disabled.

Configuring multicast source port filtering on a port or a group of ports

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Enable multicast source port filtering.	**igmp-snooping source-deny**	Required. Defaults to disabled.

When enabled to filter IPv4 multicast data based on the source ports, some device models are automatically enabled to filter IPv6 multicast data based on the source ports.

Configuring the function of 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 the VLAN to which the unknown multicast data belongs with unknown multicast data, 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.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Enable the function of dropping unknown multicast data.	**igmp-snooping drop-unknown**	Required. Defaults to disabled.

Configuring IGMP report suppression

When a Layer 2 device receives an IGMP report from a multicast group member, the device forwards the message to the Layer 3 device directly connected with it. When multiple members of a multicast group are attached to the Layer 2 device, the Layer 3 device directly connected with it will receive duplicate IGMP reports from these members.

With the IGMP report suppression function enabled, within each query cycle, the Layer 2 device forwards only the first IGMP report per multicast group to the Layer 3 device and will not forward the subsequent IGMP reports from the same multicast group to the Layer 3 device. This helps reduce the number of packets being transmitted over the network.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IGMP snooping view.	**igmp-snooping**	—

To do...	Use the command...	Remarks
3. Enable IGMP report suppression.	**report-aggregation**	Optional. Defaults to enabled.

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.

Configuring maximum multicast groups that can be joined on a port

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

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Configure the maximum number of multicast groups allowed on the port.	**igmp-snooping group-limit** *limit* [**vlan** *vlan-list*]	Optional. • 4000 by default for A5800 Switch Series. • 2000 by default for A5820X Switch Series

When the number of multicast groups that a port has joined reaches the maximum number configured, the system deletes all the forwarding entries persistent to that port from the IGMP snooping forwarding table, and the hosts on this port must join the multicast groups again.

If you have configured static or simulated joins on a port, when the number of multicast groups on the port exceeds the configured threshold, the system deletes all the forwarding entries persistent to that port from the IGMP snooping forwarding table. The system then applies the static or simulated joins again, until the number of multicast groups joined by the port comes back within the configured threshold.

Configuring multicast group replacement

The number of multicast groups that can be joined on the current switch or a port might exceed the upper limit for the switch or the port. In some specific applications, a multicast group newly joined on the switch must replace an existing multicast group automatically. A typical example is channel switching where, to join a new multicast group, a user switches from the current multicast group to a new one.

To address such situations, enable the multicast group replacement function on the switch or on certain ports. When the number of multicast groups joined on the switch or on a port reaches the limit, one of the following occurs:

- If the multicast group replacement feature is enabled, the newly joined multicast group automatically replaces an existing multicast group with the lowest address.
- If the multicast group replacement feature is not enabled, new IGMP reports are automatically discarded.

Configuring multicast group replacement globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IGMP snooping view.	**igmp-snooping**	—
3. Enable multicast group replacement.	**overflow-replace** [**vlan** *vlan-list*]	Required. Defaults to disabled.

Configuring multicast group replacement on a port or a group of ports

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Enable multicast group replacement.	**igmp-snooping overflow-replace** [**vlan** *vlan-list*]	Required. Defaults to disabled.

Be sure to configure the maximum number of multicast groups allowed on a port (see) before enabling multicast group replacement. Otherwise, the multicast group replacement functionality will not take effect.

Statically configured multicast groups cannot be replaced.

Configuring 802.1p precedence for IGMP messages

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

Configuring 802.1p precedence for IGMP messages globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IGMP snooping view.	**igmp-snooping**	—
3. Configure 802.1p precedence for IGMP messages.	**dot1p-priority** *priority-number*	Required. The default 802.1p precedence for IGMP messages is 0.

Configuring 802.1p precedence for IGMP messages in a VLAN

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—

To do...	Use the command...	Remarks
3. Configure 802.1p precedence for IGMP messages in the VLAN.	**igmp-snooping dot1p-priority** *priority-number*	Required. 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.

- Upon receiving an IGMP report from a host, the access switch checks the multicast group address and multicast source address carried in the report against 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.
- Upon 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.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Create a user profile and enter its view.	**user-profile** *profile-name*	—
3. Configure a multicast user control policy.	**igmp-snooping access-policy** *acl-number*	Required. No policy is configured by default. A host can join or leave a valid multicast group at any time.
4. Return to system view.	**quit**	—
5. Enable the created user profile.	**user-profile** *profile-name* **enable**	Required. Defaults to disabled.

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

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

Displaying and maintaining IGMP snooping

To do...	Use the command...	Remarks
Display IGMP snooping group information.	**display igmp-snooping group** [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the statistics information of IGMP messages learned by IGMP snooping.	**display igmp-snooping statistics** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display static multicast MAC address entries.	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Remove all the dynamic group entries of a specified IGMP snooping group or all IGMP snooping groups.	**reset igmp-snooping group** { *group-address* | **all** } [**vlan** *vlan-id*]	Available in user view.
Clear the statistics information of all kinds of IGMP messages learned by IGMP snooping.	**reset igmp-snooping statistics**	Available in user view.

The **reset igmp-snooping group** command works only on an IGMP snooping–enabled VLAN, but not on a VLAN with IGMP enabled on its VLAN interface.

The **reset igmp-snooping group** command cannot clear the IGMP snooping multicast group information for static joins.

IGMP snooping configuration examples

By default, Ethernet interfaces, VLAN interfaces, and aggregate interfaces are in the state of DOWN. To configure such an interface, first use the **undo shutdown** command to make the interface appear.

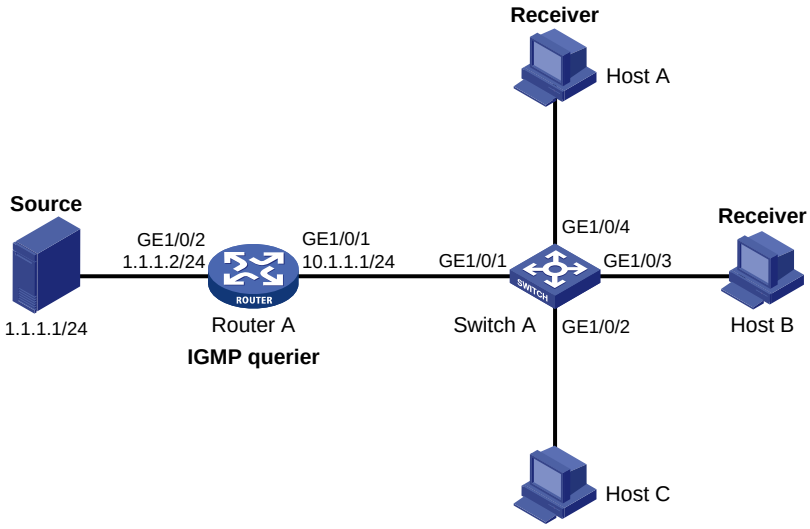
Group policy and simulated joining configuration example

Network requirements

As shown in Figure 14, Router A connects to the multicast source through GigabitEthernet 1/0/2 and to Switch A through GigabitEthernet 1/0/1. IGMPv2 is required on Router A, IGMPv2 snooping is required on Switch A, and Router A acts as the IGMP querier on the subnet.

The receivers, Host A and Host B, attached to Switch A 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.

Figure 14 Network diagram for group policy simulated joining configuration



Procedure

1. Configure an IP address and subnet mask for each interface as shown in Figure 14. The detailed configuration steps are omitted.
2. Configure Router A

Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on GigabitEthernet 1/0/1.

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

4. Verify the configuration

Display the information of the IGMP snooping groups 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
  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

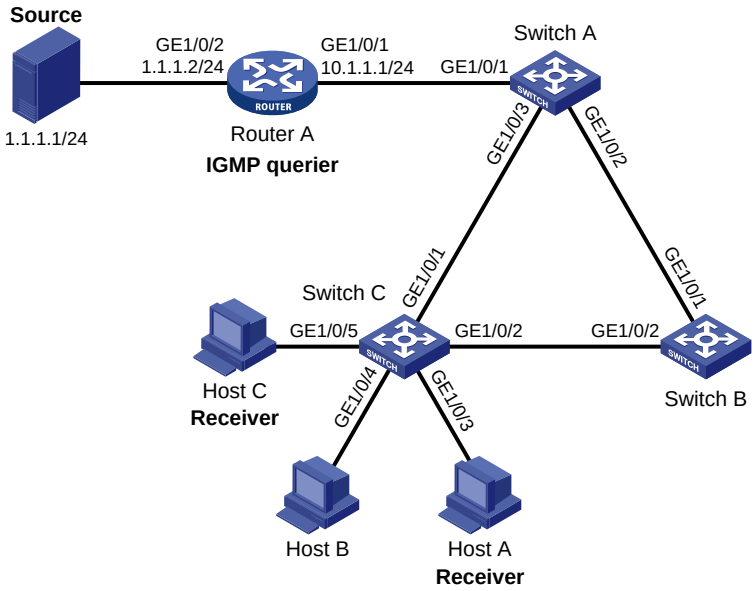
Network requirements

- As shown in Figure 15, Router A connects to a multicast source (Source) through GigabitEthernet 1/0/2, and to Switch A through GigabitEthernet 1/0/1.
- IGMPv2 will run on Router A, and IGMPv2 snooping will run on Switch A, Switch B and Switch C, with Router A acting 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 that connects Switch A to Switch C as a static router port, so that multicast traffic can flow to the receivers nearly uninterrupted along the path of Switch A—Switch C if the path Switch A—Switch B—Switch C is blocked.

If you do not configure a static router port and the path of Swtich A—Switch B— Switch C becomes 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 (multicast delivery is interrupted during this process).

For more information about STP, see *Layer 2 – LAN Switching Configuration Guide*.

Figure 15 Figure Network diagram for static port configuration



Procedure

1. Configure an IP address and subnet mask for each interface as shown in Figure 15. The detailed configuration steps are omitted.
2. Configure Router A

Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on GigabitEthernet 1/0/1.

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

6. Verify the configuration

Display the 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
  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 the 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
```

```
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
```

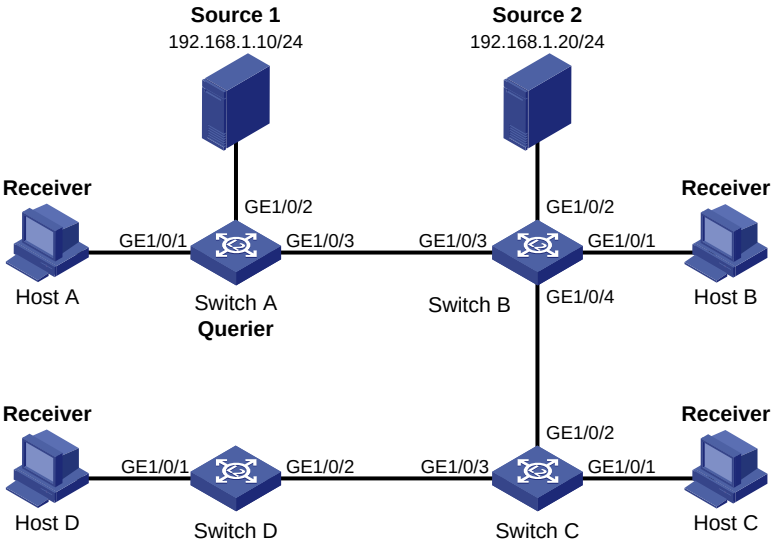
The output shows that GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 on Switch C have become static member ports for multicast group 224.1.1.1.

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 are running IGMPv2, and all the switches need to 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, 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 the default source IP address of 0.0.0.0 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 for IGMP snooping querier 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.

3. Verify the configuration

After the IGMP snooping querier starts to work, all the switches but the querier can receive IGMP general queries. Use the **display igmp-snooping statistics** command to view the statistics information about the IGMP messages received.

Display the 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.
```

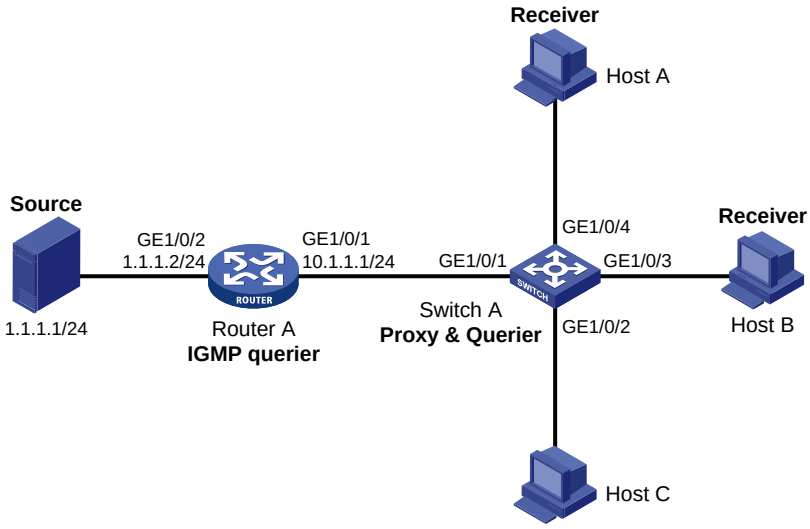
IGMP snooping proxying configuration example

Network requirements

As shown in Figure 17, Router A connects to a multicast source through port GigabitEthernet 1/0/2, and to Switch A through port GigabitEthernet 1/0/1. Router A runs IGMPv2 and Switch A runs IGMPv2 snooping. Router A serves as an 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 for IGMP snooping proxying configuration



Procedure

1. Configure an IP address and subnet mask for each interface as shown in Figure 17. The configuration steps are omitted here.
2. Configure Router A

Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on GigabitEthernet 1/0/1.

```
<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
```

4. Verify 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 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
  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 1/0/3 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).
```

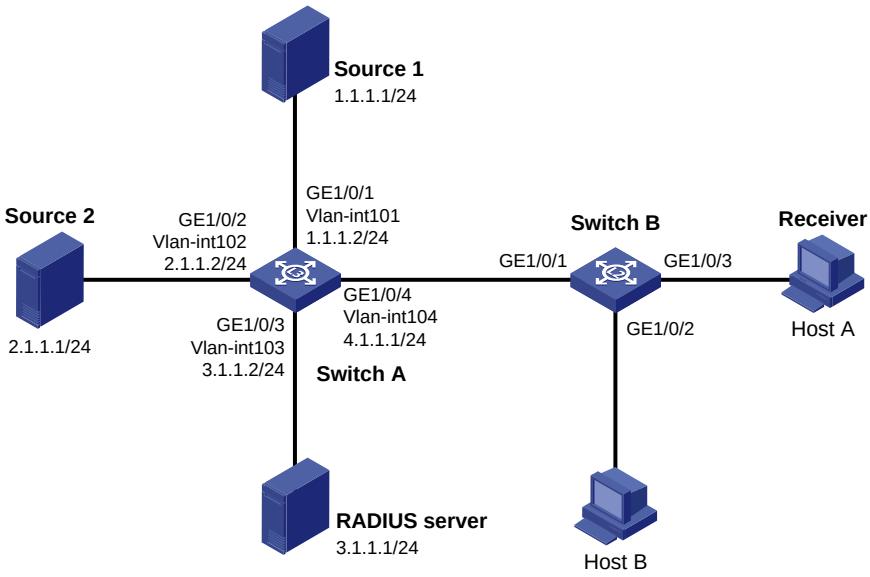
```
Total 1 MAC Group(s).
Port flags: D-Dynamic port, S-Static port, C-Copy port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 1 port.
          GE1/0/1                 (D) ( 00:01:23 )
  IP group(s):the 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.
          GE1/0/4                 (D)
  MAC group(s):
    MAC group address:0100-5e01-0101
        Host port(s):total 1 port.
          GE1/0/4
```

Multicast source and user control policy configuration example

Network requirements

- As shown in Figure 18, Switch A is a Layer-3 switch. It connects to multicast sources 1 and 2 and through VLAN-interface 101 and VLAN-interface 102 respectively. It connects to the RADIUS server through VLAN-interface 103 and to Layer-2 switch B through VLAN-interface 104.
- 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 for multicast source/user control policy configuration



Procedure

1. Configure an IP address and subnet mask for each interface as shown in Figure 18. The configuration steps are omitted here.
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
```

When configuring a multicast source control policy, you need to apply an advanced ACL to match both the multicast source address and destination address. Otherwise, multicast packets expected to be filtered out will still be forwarded.

```
[SwitchA] traffic classifier classifier1
[SwitchA-classifier-classifier1] if-match acl 3001
[SwitchA-classifier-classifier1] quit
```

Do not reference any IPv6 ACL after an IPv4 ACL is referenced in classifier view. Otherwise, match errors will occur.

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

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

5. Verify 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 100 on Switch B.

```
[SwitchB] 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
  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 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 the 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 to forward packets from Source 2 to 224.1.1.1, which indicates that multicast packets from Source 2 are blocked.

Troubleshooting IGMP snooping configuration

Switch fails in layer 2 multicast forwarding

Symptom

A switch fails to implement Layer 2 multicast forwarding.

Analysis

IGMP snooping is not enabled.

Solution

1. Enter the **display current-configuration** command to view the running status of IGMP snooping.

- If IGMP snooping is not enabled, use the igmp-snooping command to enable IGMP snooping globally, and then use igmp-snooping enable command to enable IGMP snooping in VLAN view.
- If IGMP snooping is disabled only for the corresponding VLAN, just 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 **display acl** to evaluate the configured ACL rule. Be sure that the ACL rule conforms to the multicast group policy to be implemented.
2. Use **display this** in IGMP snooping view or in the corresponding interface view to determine whether the correct multicast group policy has been applied. If not, use **group-policy** or **igmp-snooping group-policy** to apply the correct multicast group policy.
3. Use **display current-configuration** to determine whether the function of dropping unknown multicast data is enabled. If not, use **igmp-snooping drop-unknown** to enable the function of dropping unknown multicast data.

Processing multicast protocol messages

With Layer 3 multicast routing enabled, an IGMP snooping switch processes multicast protocol messages differently under different conditions.

1. With only IGMP enabled, or with both IGMP and PIM enabled on the switch, the switch:
   - Maintains dynamic member ports or dynamic router ports according to IGMP packets.
   - Maintains dynamic router ports according to PIM hello packets.
2. With only PIM enabled on the switch:
   - The switch broadcasts IGMP messages as unknown messages in the VLAN.
   - Upon receiving a PIM hello message, the switch will maintain the corresponding dynamic router port.
3. With IGMP disabled on the switch:
   - 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 without deleting its dynamic router ports.

On a switch with Layer-3 multicast routing enabled, use **display igmp group port-info** to view Layer-2 port information. For more information about this command, see *IP Multicast Command Reference*.

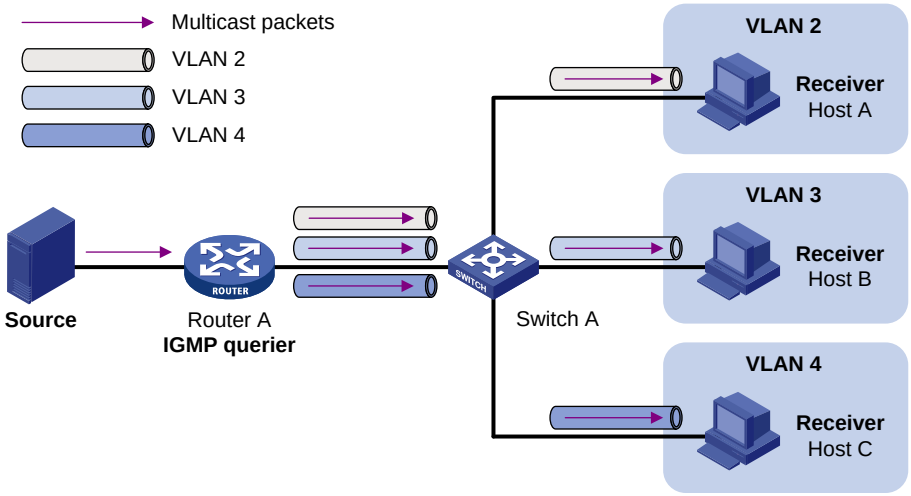
4. When PIM is disabled on the switch:
   - If IGMP is disabled, the switch deletes all its dynamic router ports.
   - If IGMP is enabled, the switch maintains all its dynamic member ports and dynamic router ports.

Configuring multicast VLAN

In this document, the switch functions as a Layer 2 device (referred to as "Switch" in network diagrams). Configurations for a Layer 3 device (referred to as "Router" in network diagrams) are implemented on an H3C router device.

In the traditional multicast programs-on-demand mode shown in Figure 19, 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 19 Multicast transmission without multicast VLAN



The multicast VLAN feature configured on the Layer 2 switch is the solution to this issue. With the multicast VLAN feature, the Layer 3 device must replicate 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.

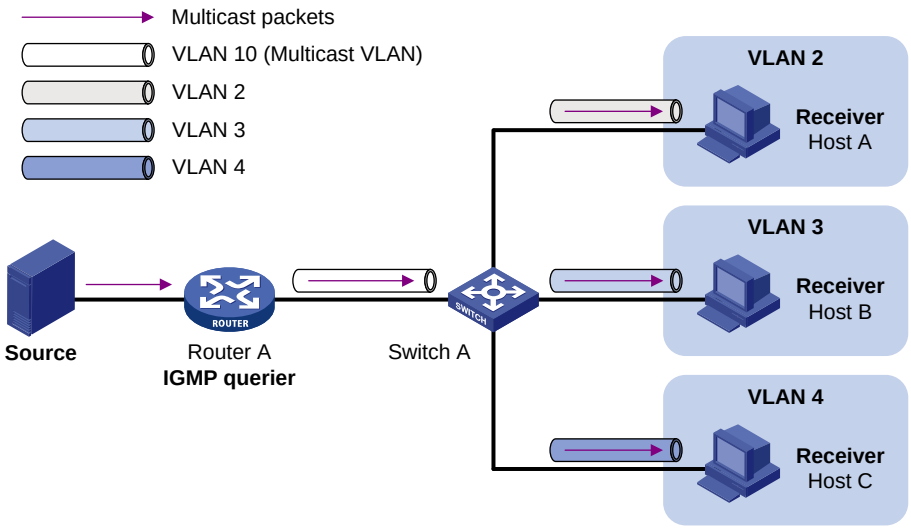
The multicast VLAN feature can be implemented using either of the following approaches.

Multicast VLAN types

Sub-VLAN-based multicast VLAN

As shown in Figure 20, Host A, Host B, and Host C are in three different user VLANs. On Switch A, configure VLAN 10 as a multicast VLAN, configure all user VLANs as sub-VLANs of this multicast VLAN, and enable IGMP snooping in the multicast VLAN.

Figure 20 Sub-VLAN-based multicast VLAN

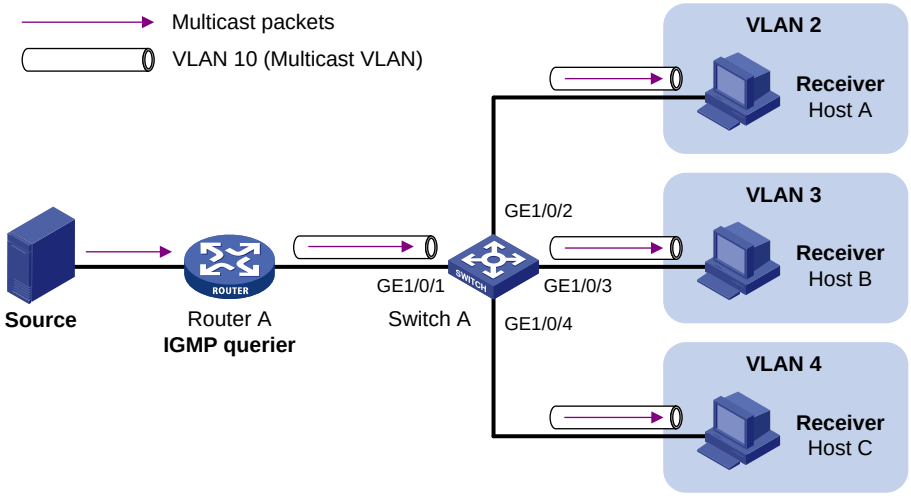


After the configuration, IGMP snooping manages router ports in the multicast VLAN and member ports in the sub-VLANs. When forwarding multicast data to Switch A, Router A needs to send only one copy of multicast traffic to Switch A in the multicast VLAN, and Switch A distributes the traffic to the multicast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

Port-based multicast VLAN

As shown in Figure 21, Host A, Host B and Host C are in three different user VLANs. All user ports (ports with attached hosts) on Switch A are hybrid ports. On Switch A, configure VLAN 10 as a multicast VLAN, assign all user ports to this multicast VLAN, and enable IGMP snooping in the multicast VLAN and all user VLANs.

Figure 21 Port-based multicast VLAN



After the configuration, upon receiving an IGMP message on a user port, Switch A tags the message with the multicast VLAN ID and relays it to the IGMP querier, so that IGMP snooping can uniformly manage the router ports and member ports in the multicast VLAN. When forwarding multicast data to Switch A, Router A needs to send only one copy of multicast traffic to Switch A in the multicast VLAN, and Switch A distributes the traffic to all member ports in the multicast VLAN.

For more information about IGMP Snooping, router ports, and member ports, see *IGMP Snooping* in the *IP Multicast Configuration Guide*.

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

Configuring sub-VLAN-based multicast VLAN

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.

Prerequisites

Before configuring 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

Procedure

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

You cannot configure multicast VLAN on a device with IP multicast routing enabled, and 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 sub-VLANs of any other multicast VLAN.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Configure the specified VLAN as a multicast VLAN and enter multicast VLAN view.	**multicast-vlan** *vlan-id*	Required. Not a multicast VLAN by default.
3. Configure the specified VLAN(s) as sub-VLAN(s) of the multicast VLAN.	**subvlan** *vlan-list*	Required. By default, a multicast VLAN has no sub-VLANs.

Configuring port-based multicast VLAN

When configuring port-based multicast VLAN, you need to 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 of the Ethernet or Layer 2 aggregate interface type.

Configurations made in Ethernet interface view are effective only for the current port. Configurations made in Layer 2 aggregate interface view are effective only for the current interface. Configurations made in port group view are effective for all the ports in the current port group.

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.

Prerequisites

Before configuring 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

Procedure

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.

Configure the user ports to permit packets of the multicast VLAN to pass and untag the packets. Thus, upon 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view or port group view.	**interface** *interface-type interface-number* **port-group** { **manual** *port-group-name* | **aggregation** *agg-id* }	Required. Use either command.
3. Configure the user port link type as hybrid.	**port link-type hybrid**	Required. Access by default.
4. Specify the user VLAN that comprises the current user port(s) as the default VLAN.	**port hybrid pvid vlan** *vlan-id*	Required. VLAN 1 by default.
5. Configure the current user port(s) to permit packets of the specified multicast VLAN(s) to pass and untag the packets.	**port hybrid vlan** *vlan-id-list* **untagged**	Required. 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 need to configure a VLAN as a multicast VLAN and then assign user ports to this multicast VLAN by either adding the user ports in the multicast VLAN or specifying the multicast VLAN on the user ports. These two configuration methods give the same result.

Configuring multicast VLAN ports in multicast VLAN view

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Configure the specified VLAN as a multicast VLAN and enter multicast VLAN view.	**multicast-vlan** *vlan-id*	Required. Not a multicast VLAN by default.

To do...	Use the command...	Remarks
3. Assign ports to the multicast VLAN.	**port** *interface-list*	Required. By default, a multicast VLAN has no ports.

Configuring multicast VLAN ports in interface view or port group view

You cannot configure multicast VLAN on a device with multicast routing enabled, and the VLAN to be configured as a multicast VLAN must exist. A port can belong to only one multicast VLAN.

To do...	Use this command...	Remarks
1. Enter system view.	**system-view**	—
2. Configure the specified VLAN as a multicast VLAN and enter multicast VLAN view.	**multicast-vlan** *vlan-id*	Required. Not a multicast VLAN by default.
3. Return to system view.	**quit**	—
4. Enter interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either command.
5. Configure the current port(s) as port(s) of the multicast VLAN.	**port multicast-vlan** *vlan-id*	Required. By default, a user port does not belong to any multicast VLAN.

Displaying and maintaining multicast VLAN

To do...	Use the command...	Remarks
Display information about a multicast VLAN.	**display multicast-vlan** [vlan-id] [| { **begin** | **exclude** | **include** } regular-expression]	Available in any view.

Multicast VLAN configuration examples

Sub-VLAN-based multicast VLAN configuration

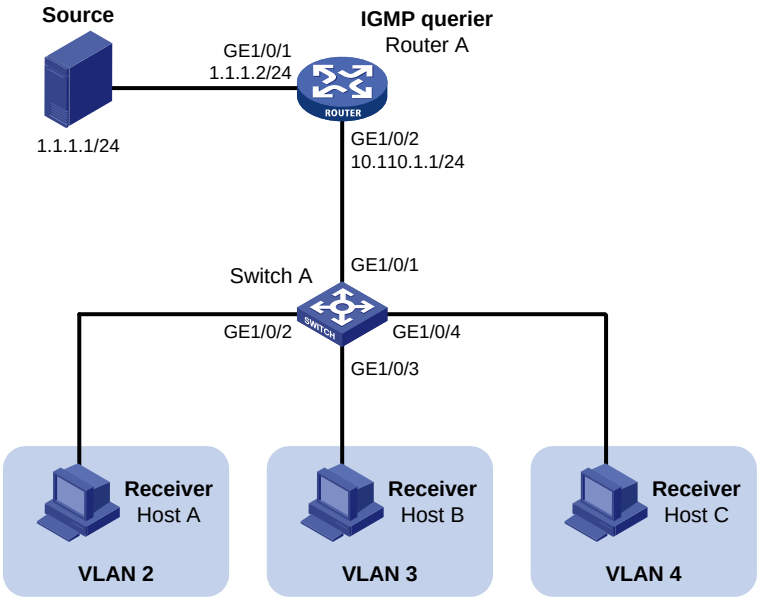
Network requirements

- Router A connects to a multicast source through GigabitEthernet1/0/1 and to Switch A, through GigabitEthernet1/0/2.
- IGMPv2 is required on Router A, and IGMPv2 snooping is required on Switch A. Router A is the IGMP querier.
- The Switch A GigabitEthernet 1/0/1 belongs to VLAN 10, GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 belong to VLAN 2 through VLAN 4 respectively, and Host A through Host C are attached to GigabitEthernet 1/0/2 through GigabitEthernet1/0/4 of Switch A respectively.
- 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.

- Configure the sub-VLAN-based multicast VLAN feature 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.

Network diagram

Figure 22 Network diagram for sub-VLAN-based multicast VLAN configuration



Procedure

1. Configure IP addresses

Configure an IP address and subnet mask for each interface as shown in Figure 22. The detailed configuration steps are omitted here.

2. Configure Router A

Enable IP multicast routing, enable PIM-DM on each interface and enable IGMP on the host-side interface GigabitEthernet1/0/2.

```
<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 and assign GigabitEthernet1/0/2 to this VLAN.

```
[SwitchA] vlan 2
```

```
[SwitchA-vlan2] port gigabitethernet 1/0/2
[SwitchA-vlan2] quit
```

The configuration for VLAN 3 and VLAN 4 is similar to the configuration for VLAN 2.

Create VLAN 10, assign GigabitEthernet1/0/1 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 4 as its sub-VLANs.

```
[SwitchA] multicast-vlan 10
[SwitchA-mvlan-10] subvlan 2 to 4
[SwitchA-mvlan-10] quit
```

4. Verify the configuration

Display information about the multicast VLAN.

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

 Multicast vlan 10
   subvlan list:
    vlan 2-4
   port list:
    no port
```

View the IGMP snooping multicast group information on Switch A.

```
[SwitchA] display igmp-snooping group
  Total 4 IP Group(s).
  Total 4 IP Source(s).
  Total 4 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy 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).
          GE1/0/3               (D)
  MAC group(s):
    MAC group address:0100-5e01-0101
        Host port(s):total 1 port(s).
          GE1/0/3

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).
          GE1/0/4               (D)
  MAC group(s):
    MAC group address:0100-5e01-0101
        Host port(s):total 1 port(s).
          GE1/0/4

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 outputs 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 4).

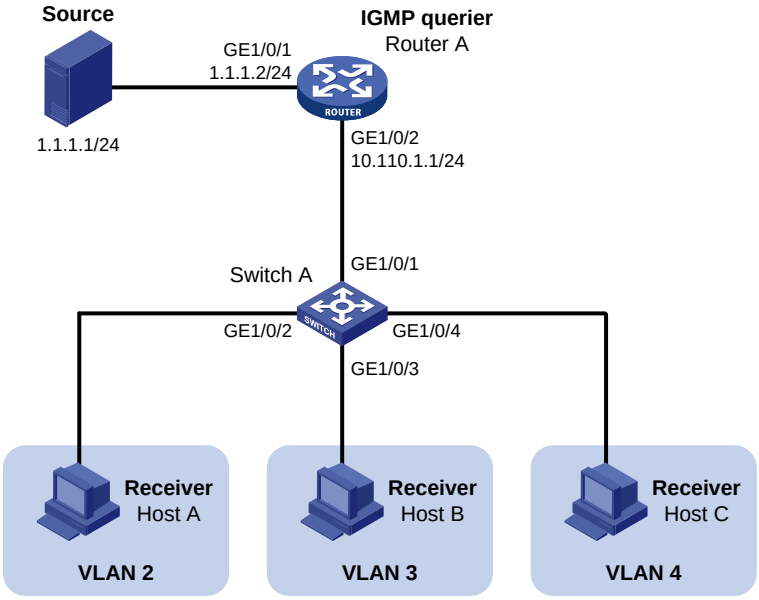
Port-based multicast VLAN configuration

Network requirements

- As shown in Figure 23, Router A connects to a multicast source (Source) through GigabitEthernet1/0/1, and to Switch A through GigabitEthernet1/0/2.
- IGMPv2 is required on Router A. IGMPv2 snooping is required on Switch A. Router A acts as the IGMP querier.
- Switch A's GigabitEthernet1/0/1 belongs to VLAN 10, GigabitEthernet1/0/2 through GigabitEthernet1/0/4 belong to VLAN 2 through VLAN 4 respectively, and Host A through Host C are attached to GigabitEthernet1/0/2 through GigabitEthernet1/0/4 of Switch A respectively.
- 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.
- Configure the port-based multicast VLAN feature 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.

Network diagram

Figure 23 Network diagram for port-based multicast VLAN configuration



Procedure

1. Configure IP addresses

Configure the IP address and subnet mask for each interface as shown in Figure 23. The detailed configuration steps are omitted here.

2. Configure Router A

Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on the host-side interface GigabitEthernet1/0/2.

```
<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 GigabitEthernet1/0/1 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. The detailed configuration steps are omitted.

Configure GigabitEthernet1/0/2 as a hybrid port. Configure VLAN 2 as the default VLAN. Configure GigabitEthernet1/0/2 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 GigabitEthernet1/0/3 and GigabitEthernet1/0/4 is similar. The detailed configuration steps are omitted.

Configure VLAN 10 as a multicast VLAN.

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

Assign GigabitEthernet1/0/2 and GigabitEthernet1/0/3 to VLAN 10.

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

Assign GigabitEthernet1/0/4 to VLAN 10.

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

4. Verify the configuration

View 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
```

View 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
  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

The interfaces in this document refer to Layer 3 interfaces in generic sense and Ethernet interfaces that operate in route mode. For more information about the operating mode of the Ethernet interfaces, see the *Layer 2—LAN Switching Configuration Guide*.

Multicast routing and forwarding overview

Multicast routing and forwarding are implemented by the following types of tables:

- 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 about different multicast routing protocols forms a general multicast routing table.
- Multicast forwarding table—The multicast forwarding table directly controls the forwarding of multicast packets.

A multicast routing table consists of a set of (S, G) entries, each indicating 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 into its multicast forwarding table.

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

Interface view mentioned in this chapter can be VLAN interface view or Layer 3 Ethernet interface view. Layer 3 Ethernet interfaces refer to Ethernet interfaces configured to operate in route mode. To switch the operating mode of an Ethernet port, see *Layer 2 - LAN Switching Configuration Guide*.

RPF check mechanism

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

RPF verification process

An RPF check is based on one of the following routing tables:

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

When performing an RPF check, a router searches its unicast routing table, MBGP routing table, and multicast static routing table at the same time. The following describes the specific process:

- The router chooses an optimal route from the unicast routing table, MBGP routing table, and multicast static 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 multicast static route by searching its multicast static 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.

- The router selects one of these three 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 three. If these 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 the RPF route according to the sequence of multicast static 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 the RPF route according to the sequence of multicast static route, MBGP route, and unicast route.

The previously mentioned *packet source* can mean different things in different situations:

For a packet traveling along the SPT from the multicast source to the receivers or the RP, the packet source for RPF verification is the multicast source.

For a packet traveling along the RPT from the RP to the receivers, the packet source for RPF verification is the RP.

For a bootstrap message from the BSR, the packet source for RPF verification is the BSR.

For more information about the concepts of SPT, RPT, and BSR, see the *IP Multicast Configuration Guide*.

Implementation of RPF check in multicast

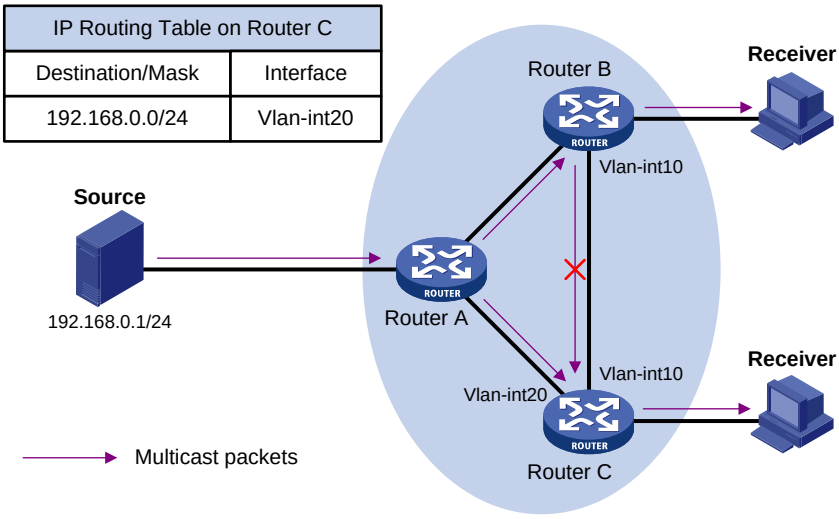
Implementing an RPF check on each received multicast data packet would bring a big burden to the router. The use of a multicast forwarding table is the solution to this issue. When creating a multicast routing entry and a multicast forwarding entry for a multicast packet, the router sets the RPF interface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

- If the corresponding (S, G) entry does not exist in the multicast forwarding table, the packet undergoes an RPF verification. 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 on which the packet arrived is the RPF interface, the RPF verification succeeds and the router forwards the packet to all the outgoing interfaces.
  - If the interface on which the packet arrived is not the RPF interface, the RPF verification fails and the router discards the packet.
- If the corresponding (S, G) entry exists, and the interface on which the packet arrived is the incoming interface, the router forwards the packet to all the outgoing interfaces.

- If the corresponding (S, G) entry exists, but the interface on which the packet arrived is not the incoming interface in the multicast forwarding table, the multicast packet undergoes an RPF verification.
  - If the RPF interface is the incoming interface of the (S, G) entry, 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, 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 unicast routes are available in the network, MBGP is not configured, and no multicast static routes have been configured on Router C, as shown in Figure 24. Multicast packets travel along the SPT from the multicast source to the receivers. The multicast forwarding table on Router C contains the (S, G) entry, with Vlan-interface20 as the incoming interface.

Figure 24 RPF check process



- When a multicast packet arrives on interface Vlan-interface20 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 a multicast packet arrives on interface Vlan-interface10 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 unicast routing table and finds that the outgoing interface to Source—the RPF interface—is Vlan-interface20. It indicates the (S, G) entry is correct and the packet arrived along a wrong path. The RPF check fails and the packet is discarded.

Multicast static routes

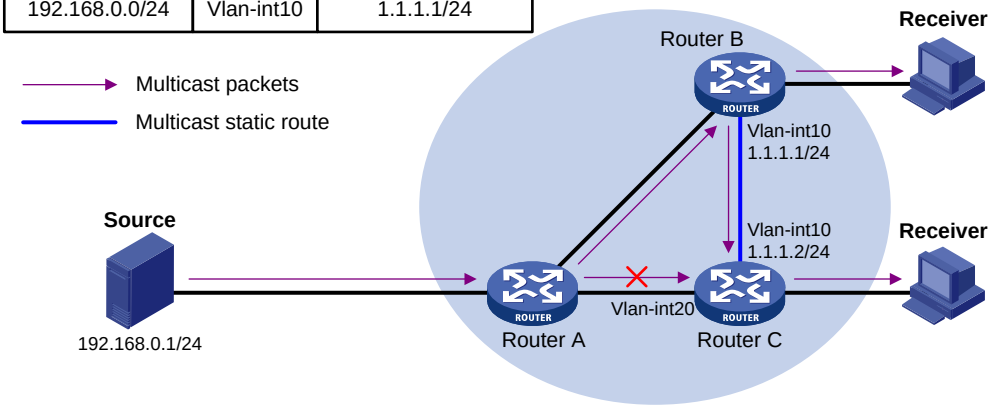
A multicast static route is an important basis for RPF verification. Depending on the application environment, the function of a multicast static route is to change an RPF route or create an RPF route.

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 that unicast traffic does. By configuring a multicast static route for a given multicast source, you can change the RPF route to create a transmission path for multicast traffic that is different from the transmission path for unicast traffic.

Figure 25 Changing an RPF route

Multicast Routing Table Static on Router C		
Source/Mask	Interface	RPF neighbor/Mask
192.168.0.0/24	Vlan-int10	1.1.1.1/24



As shown in Figure 25, when no multicast static route is configured, Router C's RPF neighbor on the path back to Source is Router A and the multicast information from Source travels along the path from Router A to Router C, which is the unicast route between the two routers; with a multicast static route configured on Router C and with Router B as Router C's RPF neighbor on the path back to Source, the multicast information from Source travels from Router A to Router B and then to Router C.

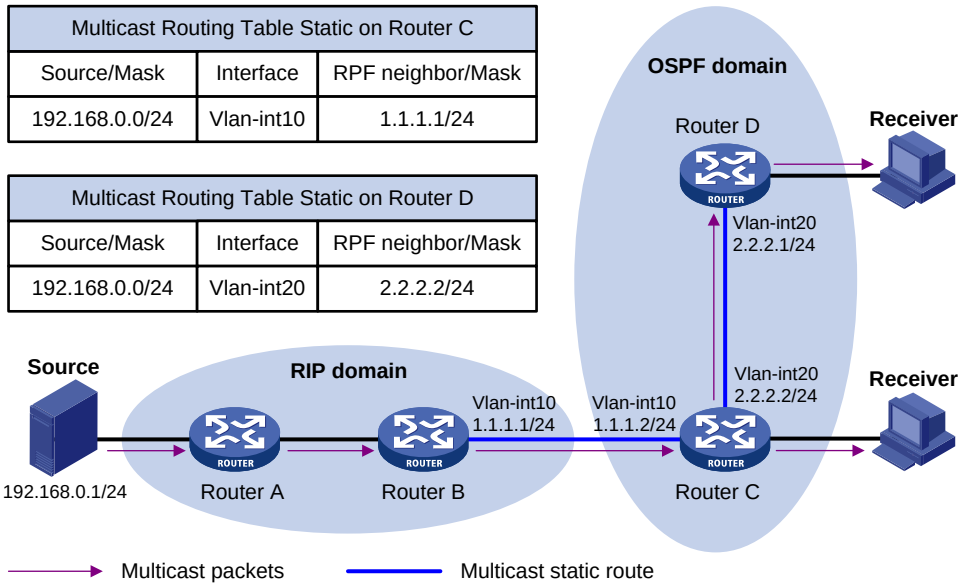
Creating an RPF route

When a unicast route is blocked, multicast traffic forwarding might be stopped because of a lack of an RPF route. By configuring a multicast static 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 26 Creating an RPF route

Multicast Routing Table Static on Router C		
Source/Mask	Interface	RPF neighbor/Mask
192.168.0.0/24	Vlan-int10	1.1.1.1/24

Multicast Routing Table Static on Router D		
Source/Mask	Interface	RPF neighbor/Mask
192.168.0.0/24	Vlan-int20	2.2.2.2/24



As shown in Figure 26, the RIP domain and the OSPF domain are unicast isolated from each other. When no multicast static route is configured, the hosts (Receiver) in the OSPF domain cannot receive the

multicast packets that the multicast source (Source) sent in the RIP domain. After you configure a multicast static route on Router C and Router D, specifying Router B as the RPF neighbor of Router C and Router C as the RPF neighbor of Router D, the receivers can receive multicast data that the multicast source sent.

A multicast static route only affects RPF verification; it cannot guide multicast forwarding. Therefore, a multicast static route is also called an "RPF static route."

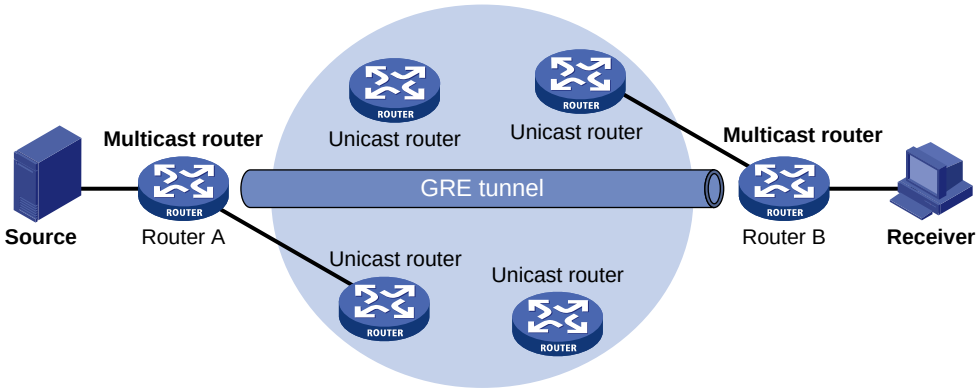
A multicast static route is effective only on the multicast switch on which it is configured, and will not be advertised throughout the network or redistributed to other routers.

Application of GRE tunnel in multicast forwarding

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 router that does not support IP multicast, the forwarding path is blocked. In this case, you can enable multicast traffic forwarding across the unicast subnet where the non-multicast-capable device resides by establishing a GRE tunnel between the devices at both ends of the unicast subnet.

For more information about GRE tunneling, see the *Layer 3 – IP Services Configuration Guide*.

Figure 27 Multicast data transmission through a GRE tunnel



As shown in Figure 27, with a GRE tunnel established between Router A and Router B, Router A encapsulates multicast data in unicast IP packets, which unicast routers then forward to Router B along the GRE tunnel. Then, Router B strips off the unicast IP header and continues forwarding 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 multicast static route across the tunnel, so that unicast cannot be transmitted through it.

Multicast traceroute

Use multicast traceroute utility to trace the path of a multicast stream 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 to that subnet, that router is called the "last-hop router."

- First-hop router—Router that directly connects to the multicast source is called the "first-hop router."
- Querier—Router that is requesting the multicast traceroute is called the "querier."

Introduction to multicast traceroute packets

A multicast traceroute packet is a special IGMP packet, which differs 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. There are three types of Multicast traceroute packets:

- Query, with the IGMP Type field set to 0x1F
- Request, with the IGMP Type field set to 0x1F
- 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. Upon 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. The last-hop router 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 forwards it through unicast to the previous hop.
4. When the first-hop router receives the request packet, it changes the packet type to indicate a response packet, and then sends the completed packet through unicast to the multicast traceroute querier.

Enabling IP multicast routing

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

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

Enabling IP multicast routing for the public network

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enable IP multicast routing.	**multicast routing-enable**	Required. Defaults to disabled.

Enabling IP multicast routing in a VPN instance

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Create a VPN instance and enter VPN instance view.	**ip vpn-instance** *vpn-instance-name*	—

To do...	Use the command...	Remarks
3. Configure a route distinguisher (RD) for the VPN instance.	**route-distinguisher** *route-distinguisher*	Required. No RD is configured by default.
4. Enable IP multicast routing.	**multicast routing-enable**	Required. Defaults to disabled.

For more information about **ip vpn-instance** and **route-distinguisher**, see *MPLS Command Reference*.

Configuring multicast routing and forwarding

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

Prerequisites

Before configuring 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 multicast static routes

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

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Configure a multicast static route.	**ip rpf-route-static** [**vpn-instance** *vpn-instance-name*] *source-address* { *mask* | *mask-length* } [*protocol* [*process-id*]] [**route-policy** *policy-name*] { *rpf-nbr-address* | *interface-type interface-number* } [**preference** *preference*] [**order** *order-number*]	Required. No multicast static route configured by default.
3. Delete multicast static 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 verification 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

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Configure the device to select the RPF route based on the longest match.	**multicast longest-match**	Required. 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. Defaults to disabled.

Configuring a multicast routing policy in a VPN instance

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VPN instance view	**ip vpn-instance** *vpn-instance-name*	—
3. Configure the device to select the RPF route based on the longest match.	**multicast longest-match**	Required. 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. Defaults to disabled.

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 define a multicast forwarding range using one of the following methods:

- Specifying boundary interfaces, which form a closed multicast forwarding area, or
- Setting the minimum time to live (TTL) value required for a multicast packet to be forwarded. Setting the minimum TTL is not supported on A5820X&A5800 series switches.

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 a multicast boundary on an interface, the interface can no longer forward multicast packets (including packets sent from the local switch) or receive multicast packets.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—

To do...	Use the command...	Remarks
3. Configure a multicast forwarding boundary.	**multicast boundary** *group-address* { *mask* | *mask-length* }	Required. No forwarding boundary by default.

Configuring the multicast forwarding table size

The router maintains the corresponding forwarding entry for each multicast packet that it receives. Excessive multicast routing entries, however, can exhaust the router's memory and cause lower router 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 will not be deleted immediately. Instead, the multicast routing protocol that is running on the router will delete them. The router will no longer install new multicast forwarding entries until the number of existing multicast forwarding entries comes down below the configured value.

When forwarding multicast traffic, the router replicates a copy of the multicast traffic for each downstream node and forwards the traffic. Thus, each of these downstream nodes forms a branch of the multicast distribution tree. You can configure the maximum number of downstream nodes (namely, the maximum number of outgoing interfaces) for a single entry in the multicast forwarding table to lessen the burden on the router 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 will not be deleted immediately. Instead, the multicast routing protocol must delete them. The router will no longer install 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

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Configure the maximum number of entries in the multicast forwarding table.	**multicast forwarding-table route-limit** *limit*	Optional. • 4000 by default for A5800 Switch Series. • 2000 by default for A5820X Switch Series.
3. Configure the maximum number of downstream nodes for a single multicast forwarding entry.	**multicast forwarding-table downstream-limit** *limit*	Optional. Defaults to 128.

Configuring the multicast forwarding table size in a VPN instance

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VPN instance view.	**ip vpn-instance** *vpn-instance-name*	—

To do...	Use the command...	Remarks
3. Configure the maximum number of entries in the multicast forwarding table.	**multicast forwarding-table route-limit** *limit*	Optional • 4000 by default for A5800 Switch Series. • 2000 by default for A5820X Switch Series.
4. Configure the maximum number of downstream nodes for a single route in the multicast forwarding table.	**multicast forwarding-table downstream-limit** *limit*	Optional. Defaults to 128.

On an A5800 series Ethernet switch:

- Without MPLS enabled, the switch can have up to 4000 multicast forwarding entries. With MPLS enabled, the switch can have up to 3000 multicast forwarding entries.
- If the number of the multicast forwarding entries on the switch is more than 3000, you cannot enable MPLS on the switch.

Tracing a multicast path

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

To do...	Use the command...	Remarks
Trace a multicast path.	**mtracert** *source-address* [[*last-hop-router-address*] *group-address*]	Required. Available in any view.

Displaying and maintaining multicast routing and forwarding

To do...	Use the command...	Remarks
Display multicast boundary information.	**display multicast** [**all-instance** | **vpn-instance** *vpn-instance-name*] **boundary** [*group-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display multicast forwarding table information.	**display multicast** [**all-instance** | **vpn-instance** *vpn-instance-name*] **forwarding-table** [*source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } } | **statistics** | **slot** *slot-number*] * [**port-info**] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

To do...	Use the command...	Remarks
Display the DF information of the multicast forwarding table.	**display multicast** [**all-instance** | **vpn-instance** *vpn-instance-name*] **forwarding-table df-info** [*rp-address*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display multicast routing table information.	**display multicast** [**all-instance** | **vpn-instance** *vpn-instance-name*] **routing-table** [*source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } }] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display information of the multicast static routing table.	**display multicast routing-table** [**all-instance** | **vpn-instance** *vpn-instance-name*] **static** [**config**] [*source-address* { *mask-length* | *mask* }] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display RPF route information of the specified multicast source.	**display multicast** [**all-instance | vpn-instance** *vpn-instance-name*] **rpf-info** *source-address* [*group-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Clear forwarding entries from the multicast forwarding table.	**reset multicast** [**all-instance | vpn-instance** *vpn-instance-name*] **forwarding-table** { { *source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }	Available in user view.
Clear routing entries from the multicast routing table.	**reset multicast** [**all-instance | vpn-instance** *vpn-instance-name*] **routing-table** { { *source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }	Available in user view.

The **reset** command clears the information in the multicast routing table or the multicast forwarding table, and thus may cause failure of multicast transmission.

When a routing entry is deleted from the multicast routing table, the corresponding forwarding entry will also be deleted from the multicast forwarding table.

When a forwarding entry is deleted from the multicast forwarding table, the corresponding routing entry will also be deleted from the multicast routing table.

Configuration examples

Changing an RPF route

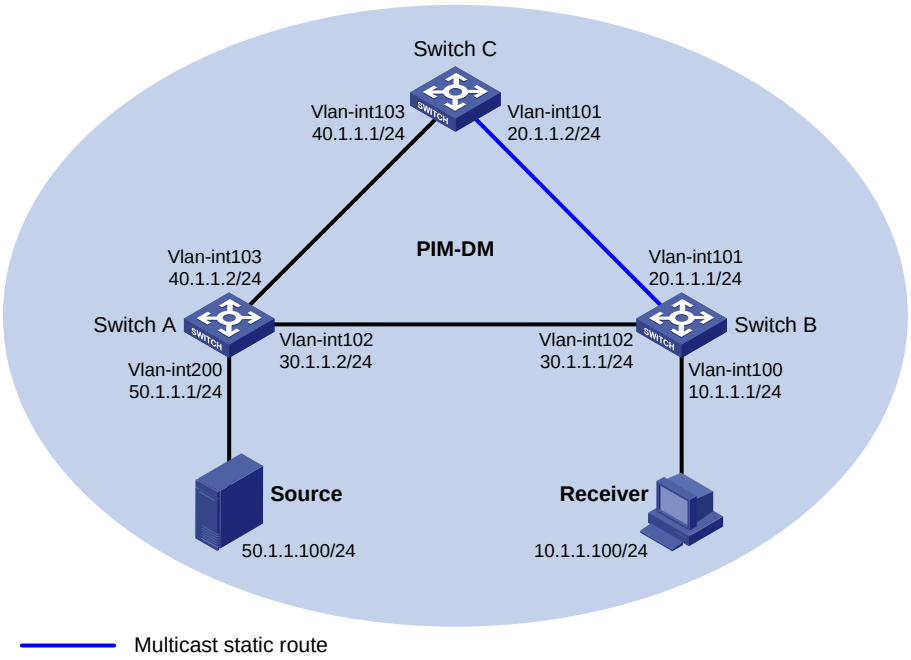
Network requirements

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

Network diagram

Figure 28 Network diagram for RPF route alternation configuration



Procedure

1. Configure IP addresses and unicast routing

Configure the IP address and subnet mask for each interface as shown in Figure 28. The detailed configuration steps are omitted here.

Enable OSPF on the switches in the PIM-DM domain. Ensure the network-layer interoperation among the switches in the PIM-DM domain. Ensure that the switches can dynamically update their routing information by leveraging the unicast routing protocol. The specific configuration steps are omitted here.

2. Enable IP multicast routing, and enable PIM-DM and IGMP

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

```
<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
```

The configuration on Switch C is similar to the configuration on Switch A. The specific configuration steps are omitted here.

Use the **display multicast rpf-info** command to view 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.

3. Configure a multicast static route

Configure a multicast static 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
```

4. Verify the configuration

Use the **display multicast rpf-info** command to view the 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: multicast static
     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 multicast static route, and the RPF neighbor is now Switch C.

Creating an RPF route

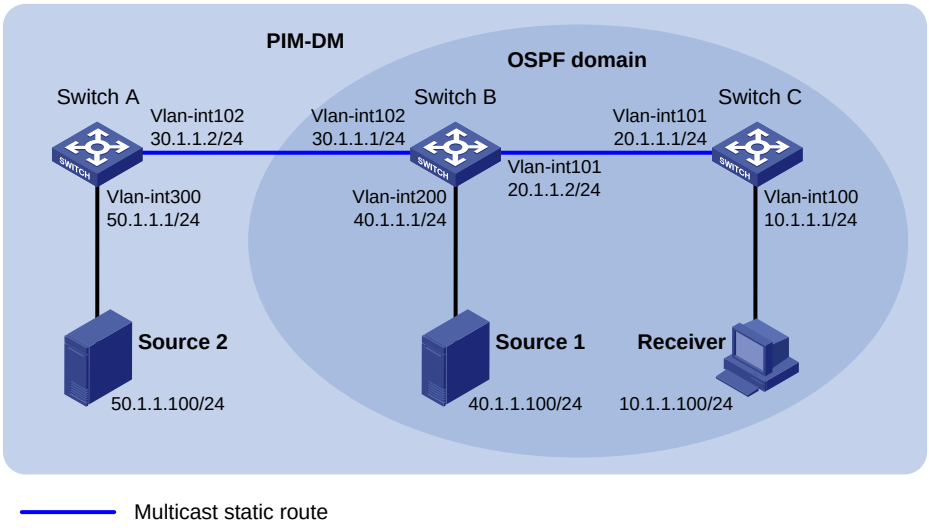
Network requirements

- 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.

- 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.

Network diagram

Figure 29 Network diagram for creating an RPF route



Procedure

1. Configure the IP address and subnet mask for each interface as shown in Figure 29. The detailed configuration steps are omitted here.
2. Enable OSPF on Switch B and Switch C. Ensure the network-layer interoperation among Switch B and Switch C. Ensure that the switches can dynamically update their routing information by leveraging the unicast routing protocol. The specific configuration steps are omitted here.
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
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] pim dm
[SwitchC-Vlan-interface300] quit
[SwitchC] interface vlan-interface 102
```

```
[SwitchC-Vlan-interface102] pim dm
[SwitchC-Vlan-interface102] quit
```

The configuration on Switch B is similar to that on Switch A. The specific configuration steps are omitted here.

Use the **display multicast rpf-info** command to view 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, indicating that no RPF route to Source 2 exists on Switch B or Switch C.

4. Configure a multicast static route

Configure a multicast static 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 multicast static 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
```

5. Verify the configuration

Use the **display multicast rpf-info** command to view 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: multicast static
     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: multicast static
     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.

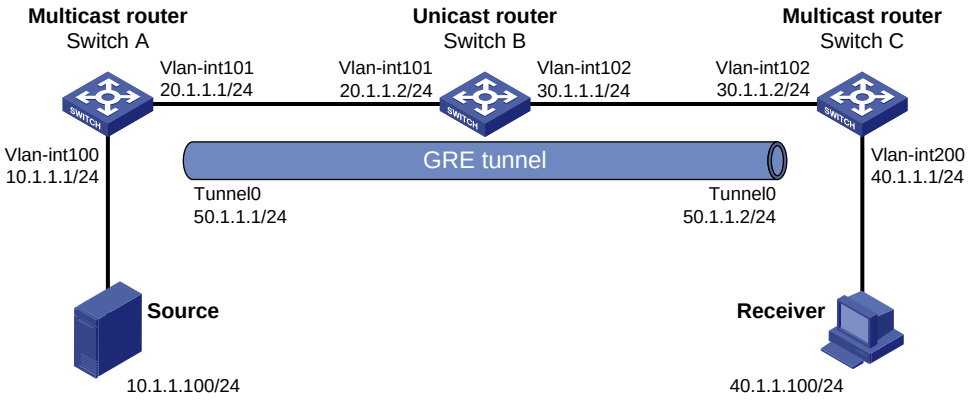
Multicast forwarding over a GRE tunnel

Network requirements

- Multicast routing and PIM-DM are enabled on Switch A and Switch C. Switch B does not support multicast.
- OSPF is running on Switch A, Switch B, and Switch C.
- Perform the following configurations so that Receiver can receive the multicast data from Source.

Network diagram

Figure 30 Network diagram for configuring multicast forwarding over a GRE tunnel



Procedure

1. Configure the IP address and subnet mask for each interface as shown in Figure 30. The detailed configuration steps are omitted here.
2. Configure a GRE tunnel

Create Tunnel 0 on Switch A and configure the IP address and subnet mask for the interface.

```
<SwitchA> system-view
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ip address 50.1.1.1 24
```

Configure Tunnel 0 to work in the GRE tunnel mode and specify the source and destination addresses for the interface.

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

Create Tunnel 0 on Switch C and configure the IP address and subnet mask for the interface.

```
<SwitchC> system-view
[SwitchC] interface tunnel 0
[SwitchC-Tunnel0] ip address 50.1.1.2 24
```

Configure Tunnel to operate in the GRE tunnel mode and configure the source and destination addresses for the interface.

```
[SwitchC-Tunnel0] tunnel-protocol gre
[SwitchC-Tunnel0] source 30.1.1.2
[SwitchC-Tunnel0] destination 20.1.1.1
[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. Configure a static multicast route

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
```

6. Verify 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. Use **display pim routing-table** to view the PIM routing table information on routers.

View 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 a GRE tunnel to Switch C.

Troubleshooting multicast routing and forwarding

Multicast static 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 multicast static route fails.

Analysis

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

Solution

1. Use **display multicast routing-table static config** to view the detailed configuration information of multicast static routes to verify that the multicast static route has been correctly configured and the route entry exists.
2. Use **display multicast routing-table static** to view the information of multicast static routes to verify that the multicast static route has been correctly configured and the route entry exists in the multicast routing table.
3. Check the type of the next hop interface of the multicast static 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 multicast static route.
4. Check that the multicast static route matches the specified routing protocol. If a protocol was specified in multicast static route configuration, enter the **display ip routing-table** command to check whether an identical route was added by the protocol.
5. Check that the multicast static route matches the specified routing policy. If a routing policy was specified when the multicast static 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 **display pim routing-table** to check whether the corresponding (S, G) entries exist on the router. If so, the router has received the multicast data. Otherwise, the router has not received the data.
2. Use **display multicast boundary** to view 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 **display current-configuration** to check the BSR and RP information.

Configuring IGMP

The interfaces in this document refer to Layer 3 interfaces in generic sense and Ethernet interfaces operating in route mode. For more information about the operating mode of the Ethernet interface, see *Layer 2—LAN Switching Configuration Guide*.

IGMP overview

As a TCP/IP protocol responsible for IP multicast group member management, IGMP is used by IP hosts to establish and maintain their multicast group memberships to immediately neighboring multicast routers.

Interface view mentioned in this chapter can be VLAN interface view or Layer 3 Ethernet interface view. Layer 3 Ethernet interfaces refer to Ethernet interfaces configured to operate in route mode. To switch the operating mode of an Ethernet port, see *Layer 2 - LAN Switching Configuration Guide*.

IGMP versions

IGMP versions are as follows:

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

All IGMP versions support the ASM model. In addition to support for the ASM model, IGMPv3 can be directly deployed to implement the SSM model, but 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 *IP Multicast Configuration Guide*.

Introduction to IGMPv1

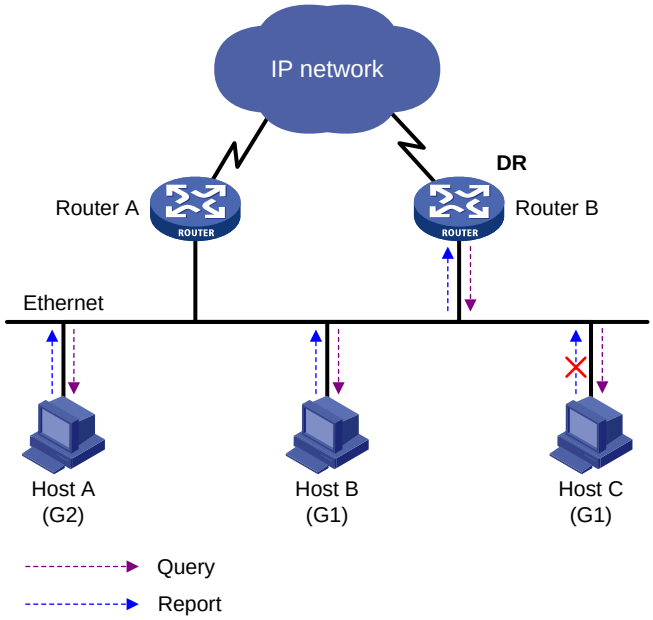
IGMPv1 manages multicast group memberships primarily based on the query and response mechanism.

All multicast routers on the same subnet can get 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 DR elected by the working multicast routing protocol (such as PIM) serves as the IGMP querier.

For more information about DR, see *PIM* in the *IP Multicast Configuration Guide*.

Figure 31 Figure IGMP queries and reports



Assume that Host B and Host C receive multicast data addressed to multicast group G1 and Host A receives multicast data addressed to G2, as shown in Figure 31. 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 will 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 determined that at least one host on the local subnet is available for G1. This mechanism, known as IGMP report suppression of the host, helps reduce traffic on the local subnet.
4. At the same time, because Host A is available for 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 (PIM, for example) that is running on the routers generates (*, G1) and (*, G2) multicast forwarding entries. These entries will be the basis for subsequent multicast forwarding, where * 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.

Because IGMPv1 does not specifically define a leave group message (often called a “leave message”), upon leaving a multicast group, an IGMPv1 host stops sending reports to the address of the multicast group that it monitored. If no member of a multicast group exists on the subnet, the IGMP router does not receive any report addressed to that multicast group, so the routers 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 host response timeout to determine whether a group has members. This adds to the leave latency.

In IGMPv2, when a host leaves a multicast group, the following process occurs:

1. The host sends a leave message to all routers on the local subnet. The destination address is 224.0.0.2.
2. Upon 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 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 assumes that no hosts on the subnet are interested in multicast traffic to that group and stops maintaining the memberships of the group.

Enhancements in IGMPv3

IGMPv3 is built on and is compatible with IGMPv1 and IGMPv2. IGMPv3 provides hosts with enhanced control capabilities and provides query and report message enhancements.

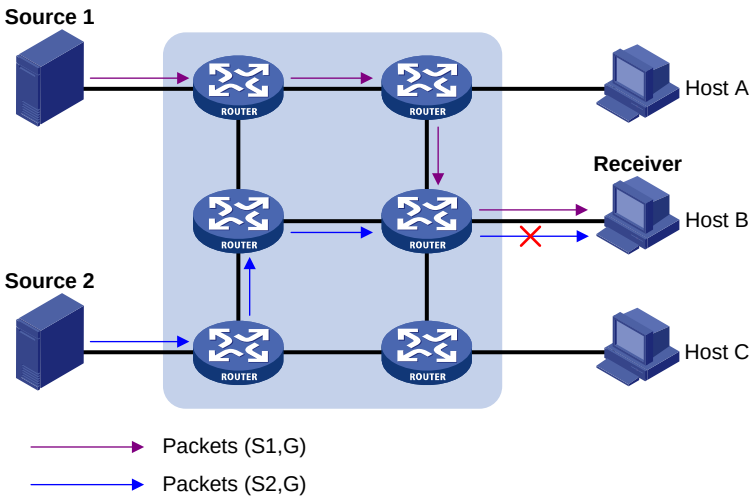
Enhancements in control capability of hosts

IGMPv3 has introduced source filtering modes (Include and Exclude), so that a host can not only join a designated multicast group, it can also specify whether to receive or reject multicast data from a designated multicast source. When a host joins a multicast group, one of the following 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 32, 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 receives the multicast data that Source 1 sends to G but not the data from Source 2.

Figure 32 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. Multicast streams from both Source 1 and Source 2 flow to Host B whether it needs them or not.

When IGMPv3 is running between the hosts and routers, Host B can explicitly express its interest in 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)). Only multicast data from Source 1 is 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 record types include the following:

- IS_IN—The source filtering mode is Include. Namely, 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. Namely, the report sender requests the multicast data from any sources but those defined in the specified multicast source list.

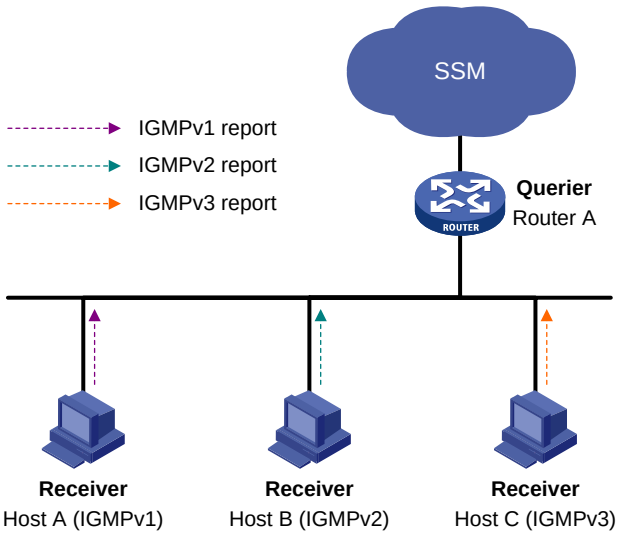
- TO_IN—The filtering mode has changed from Exclude to Include.
- TO_EX—The filtering mode has changed from Include to Exclude.
- ALLOW—The Source Address fields in this group record contain a list of the additional sources that the system will obtain data from, for packets sent to the specified multicast address. If the change was made to an Include source list, these sources are the addresses that were added to the list. If the change was made 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 will no longer obtain data from, for packets sent to the specified multicast address. If the change was made to an Include source list, these sources are the addresses that were deleted from the list. If the change was made to an Exclude source list, these sources are the addresses that were added to the list.

IGMP SSM mapping

The IGMP SSM mapping feature allows 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 is aware of 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 33 Network diagram for IGMP SSM mapping



As shown in Figure 33, 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 while it is infeasible to run IGMPv3 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 determines the multicast group address G carried in the message.

- 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.

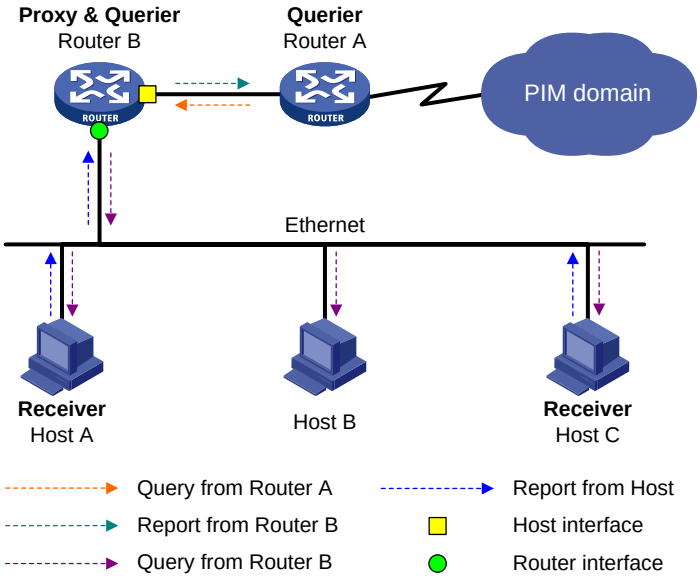
The IGMP SSM mapping feature does not process IGMPv3 reports.

For more information about the SSM group range, see the *IP Multicast Configuration Guide*.

IGMP proxying

In some simple tree 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 configured with IGMP proxying is a host but no longer a PIM neighbor to the upstream device.

Figure 34 Network diagram for IGMP proxying



As shown in Figure 34, 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. 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. 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.

Multi-instance IGMP

While IGMP maintains group memberships on a per-interface basis, IGMP in a VPN instance handles protocol packets based on the VPN instance on the interface. Upon receiving an IGMP packet, the router determines the instance to which the message belongs and handles the message within the instance. If IGMP running in a VPN instance needs to exchange information with another multicast protocol, the router informs the other multicast protocol only within the VPN instance.

Protocols and standards

The following documents describe different IGMP versions:

- 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")*

Configuring basic functions of IGMP

Prerequisites

Before configuring the basic functions of IGMP, 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 rules for multicast group filtering
- Determine the maximum number of multicast groups that an interface can joined

Enabling IGMP

To configure IGMP, enable IGMP on the interface on which the multicast group memberships will be established and maintained. All other configuration tasks are optional.

Enabling IGMP for the public network

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enable IP multicast routing.	**multicast routing-enable**	Required. Defaults to disabled.
3. Enter interface view.	**interface** *interface-type interface-number*	—
4. Enable IGMP.	**igmp enable**	Required. Defaults to disabled.

Enabling IGMP in a VPN instance

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Create a VPN instance and enter VPN instance view.	**ip vpn-instance** *vpn-instance-name*	—
3. Configure an RD for the VPN instance.	**route-distinguisher** *route-distinguisher*	Required. No RD is configured by default.
4. Enable IP multicast routing.	**multicast routing-enable**	Required. Defaults to disabled.
5. Enter interface view.	**interface** *interface-type interface-number*	—
6. Associate the current interface with the VPN instance.	**ip binding vpn-instance** *vpn-instance-name*	Required. No VPN instance is associated with an interface by default.
7. Enable IGMP.	**igmp enable**	Required. Defaults to disabled.

For more information about the **ip vpn-instance**, **route-distinguisher** and **ip binding vpn-instance** commands, see *MPLS L3VPN* in the *MPLS Command Reference*.

For more information about the **multicast routing-enable** command, see *Multicast Routing and Forwarding* in the *IP Multicast 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

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network IGMP view or VPN instance IGMP view.	**igmp** [**vpn-instance** *vpn-instance-name*]	—

To do...	Use the command...	Remarks
3. Configure an IGMP version globally.	**version** *version-number*	Optional. Defaults to IGMPv2.

Configuring an IGMP version on an interface

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure an IGMP version on the interface.	**igmp version** *version-number*	Optional. Defaults to IGMPv2.

Configuring static joining

After an interface is configured as a static member of a multicast group or a multicast source group, it acts 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.

Follow these steps to configure an interface as a statically connected member of a multicast group or a multicast source and group:

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure the interface as a static member of a multicast group or a multicast source and group.	**igmp static-group** *group-address* [**source** *source-address*]	Required. An interface is not a static member of any multicast group or multicast source and group by default.

Before you can configure an interface of a PIM-SM device 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 this interface is IGMP enabled but not PIM-SM enabled, it must be an IGMP querier. For more information about PIM-SM and a DR, see *PIM* in the *IP Multicast Configuration Guide*.

As a static member of a multicast group or a multicast source and group, the interface does not respond to the queries from the IGMP querier, nor does it send an unsolicited IGMP membership report or an IGMP leave group message when it joins or leaves a multicast group or a multicast source and group. In other words, the interface will not become a real member of the multicast group or the multicast source and group.

Configuring a multicast group filter

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

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure a multicast group filter.	**igmp group-policy** *acl-number* [*version-number*]	Required. By default, no multicast group filter is configured on this interface. The hosts on the current interface can join any valid multicast group.

Configuring the maximum number of multicast groups on an interface

You can configure the allowed maximum number of multicast groups on an interface to flexibly control the number of multicast groups the interface can join.

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Configure the maximum number of multicast groups that the current interface can join	**igmp group-limit** *limit*	Required • 4000 by default for A5800 Switch Series. • 2000 by default for A5820X Switch Series.

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

Adjusting IGMP performance

Configurations performed in IGMP view are effective on all interfaces, while configurations performed in interface view are effective on the current interface only. If the same feature is configured in both IGMP view and interface view, the configuration performed in interface view is given priority, regardless of the configuration sequence.

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 functions of IGMP.
- 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.

Configuring IGMP message options

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

Configuring IGMP packet options globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network IGMP view or VPN instance IGMP view.	**igmp** [**vpn-instance** *vpn-instance-name*]	—
3. Configure the router to discard any IGMP message that does not carry the Router-Alert option.	**require-router-alert**	Optional. By default, the device does not check the Router-Alert option.
4. Enable insertion of the Router-Alert option into IGMP messages.	**send-router-alert**	Optional. By default, IGMP messages carry the Router-Alert option.

Configuring IGMP packet options on an interface

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure the interface to discard any IGMP message that does not carry the Router-Alert option.	**igmp require-router-alert**	Optional. By default, the device does not check the Router-Alert option.

To do...	Use the command...	Remarks
4. Enable insertion of the Router-Alert option into IGMP messages.	**igmp send-router-alert**	Optional. By default, IGMP messages carry the Router-Alert option.

Configuring IGMP query and response parameters

The IGMP querier robustness variable defines the maximum number of attempts for transmitting IGMP general queries, group-specific queries, or group-and-source-specific queries in case of packet loss due to network problems. A greater value of the robustness variable makes the IGMP querier more robust, but results in longer multicast group timeout time.

On startup, the IGMPv1/v2/v3 querier sends **startup query count** IGMP general queries at the **startup query interval**.

The IGMPv1/v2/v3 querier periodically sends IGMP general queries at the **IGMP general query interval** to determine whether any multicast group member exists on the network. You can tune the IGMP general query interval based on actual condition of the network.

After receiving an IGMP leave message, the IGMPv2 querier sends **last-member query count** IGMP group-specific queries at the **IGMP last-member query interval**. After receiving an IGMP report that tells relation changes between multicast groups and multicast sources, the IGMPv3 querier sends **last-member query count** IGMP group-and-source-specific queries at the **IGMP last-member query interval**. The value of the **last-member query count** equals the value of the robustness variable.

After receiving an IGMP query (general query, group-specific query, or group-and-source-specific query), a host starts a delay timer for each multicast group it has joined. This timer is initialized to a random value in the range of 0 to the maximum response time, which is derived from the Max Response Time field in the IGMP query. When the timer value comes down to 0, the host sends an IGMP report to the corresponding multicast group.

An appropriate setting for the maximum response time for IGMP queries allows hosts to respond to queries quickly. This avoids bursts of IGMP traffic on the network caused by reports that are sent simultaneously by a large number of hosts when the corresponding timers expire.

- For IGMP general queries, configure the maximum response time to fill their Max Response time field.
- For IGMP group-specific queries and IGMP group-and-source-specific queries, configure the IGMP last-member query interval to fill their Max Response time field. For IGMP group-specific queries and IGMP group-and-source-specific queries, the maximum response time equals to 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 within the "other querier present interval", it will assume the querier to have expired and a new querier election process is launched. Otherwise, the non-querier router resets its **other querier present timer**.

Configuring IGMP query and response parameters globally

To do...	Use the command...	Remarks
1. Enter system view	**system-view**	—

To do...	Use the command...	Remarks
2. Enter public network IGMP view or VPN instance IGMP view	**igmp** [**vpn-instance** *vpn-instance-name*]	—
3. Configure the IGMP querier's robustness variable	**robust-count** *robust-value*	Optional 2 by default
4. Configure the startup query interval	**startup-query-interval** *interval*	Optional By default, the startup query interval is 1/4 of the **IGMP general query interval**.
5. Configure the startup query count	**startup-query-count** *value*	Optional By default, the startup query count is set to the IGMP querier robustness variable.
6. Configure the IGMP general query interval	**timer query** *interval*	Optional Defaults to 60 seconds.
7. Configure the maximum response time for IGMP general queries.	**max-response-time** *interval*	Optional. 10 seconds by default.
8. Configure the IGMP last-member query interval.	**last-member-query-interval** *interval*	Optional. 1 second by default.
9. Configure the other querier present interval.	**timer other-querier-present** *interval*	Optional. 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 query and response parameters on an interface

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure the IGMP querier's robustness variable.	**igmp robust-count** *robust-value*	Optional. 2 by default.
4. Configure the startup query interval.	**igmp startup-query-interval** *interval*	Optional. 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** *value*	Optional. By default, the startup query count is set to the IGMP querier's robustness variable.

To do...	Use the command...	Remarks
6. Configure the IGMP general query interval.	**igmp timer query** *interval*	Optional. Defaults to 60 seconds.
7. Configure the maximum response time for IGMP general queries.	**igmp max-response-time** *interval*	Optional. 10 seconds by default.
8. Configure the IGMP last member query interval.	**igmp last-member-query-interval** *interval*	Optional. 1 second by default.
9. Configure the other querier present interval.	**igmp timer other-querier-present** *interval*	Optional. By default, the other querier present interval is [IGMP general query interval] × [IGMP robustness variable] + [maximum response time for IGMP general queries] / 2.

Make sure that the other querier present interval is greater than the IGMP general query interval; otherwise the IGMP querier may change frequently on the network.

Make sure that the IGMP general query interval is greater than the maximum response time for IGMP general queries; otherwise, multicast group members may 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.

Configuring IGMP fast leave processing

IGMP fast leave processing is implemented by IGMP snooping. For more information, see "IGMP snooping configuration."

Configuring IGMP SSM mapping

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

Prerequisites

Before configuring 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 functions of IGMP.

Enabling SSM mapping

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—

To do...	Use the command...	Remarks
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Enable the IGMP SSM mapping feature.	**igmp ssm-mapping enable**	Required. Defaults to disabled.

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.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network IGMP view or VPN instance IGMP view.	**igmp** [**vpn-instance** *vpn-instance-name*]	—
3. Configure an IGMP SSM mapping.	**ssm-mapping** *group-address* { *mask* | *mask-length* } *source-address*	Required. No IGMP mappings are configured by default.

If IGMPv3 is enabled on a VLAN interface, 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 configuring simulated joining with **igmp-snooping host-join**. In this case, the corresponding multicast group is not created based on the configured IGMP SSM mappings. For more information about the **igmp-snooping host-join** command, see *IP Multicast Command Reference*.

Configuring IGMP proxying

Prerequisites

Before configuring 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 device serve as an IGMP proxy.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—

To do...	Use the command...	Remarks
3. Enable the IGMP proxying feature.	**igmp proxying enable**	Required. Defaults to disabled.

Each device 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.

Configuring multicast forwarding on a downstream interface

Typically, only queriers can forward multicast traffic and non-queriers have no multicast forwarding capabilities, to avoid duplicate multicast flows. It is the same on IGMP proxy devices. Only the downstream interfaces acting as a querier can forward multicast traffic to downstream hosts.

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

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Enable multicast forwarding on a non-querier downstream interface.	**igmp proxying forwarding**	Required. Defaults to disabled.

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

Displaying and maintaining IGMP

To do...	Use the command...	
Display IGMP group information.	**display igmp** [**all-instance** | **vpn-instance** *vpn-instance-name*] **group** [*group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

To do...	Use the command...	
Display the Layer 2 port information of IGMP groups.	**display igmp group port-info** [**vlan** *vlan-id*] [**chassis** *chassis-number* **slot** *slot-number*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IGMP configuration and operation information.	**display igmp** [**all-instance** | **vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the information of IGMP proxying groups.	**display igmp** [**all-instance** | **vpn-instance** *vpn-instance-name*] **proxying group** [*group-address*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display information in the IGMP routing table.	**display igmp** [**all-instance** | **vpn-instance** *vpn-instance-name*] **routing-table** [*source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **flags** { **act** | **suc** }] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IGMP SSM mappings.	**display igmp** [**all-instance** | **vpn-instance** *vpn-instance-name*] **ssm-mapping** *group-address* [**|** { **begin** | **exclude** | **include** } *regular-expression*]	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** *vpn-instance-name*] **ssm-mapping group** [*group-address* | **interface** *interface-type interface-number*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Remove all the dynamic IGMP group entries of a specified IGMP group or all IGMP groups.	**reset igmp** [**all-instance** | **vpn-instance** *vpn-instance-name*] **group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *mask* | *mask-length* }] [*source-address* [**mask** { *mask* | *mask-length* }]] } }	Available in user view.
Remove all the dynamic Layer 2 port entries of a specified IGMP group or all IGMP groups.	**reset igmp group port-info** { **all** | *group-address* } [**vlan** *vlan-id*]	Available in user view.
Clear IGMP SSM mappings.	**reset igmp** [**all-instance** | **vpn-instance** *vpn-instance-name*] **ssm-mapping group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *mask* | *mask-length* }] [*source-address* [**mask** { *mask* | *mask-length* }]] } }	Available in user view.

The **reset igmp group** command cannot remove static IGMP group entries and can cause an interruption of receiver reception of multicast data.

The **reset igmp group port-info** command cannot remove the static Layer 2 port entries of IGMP groups.

IGMP configuration examples

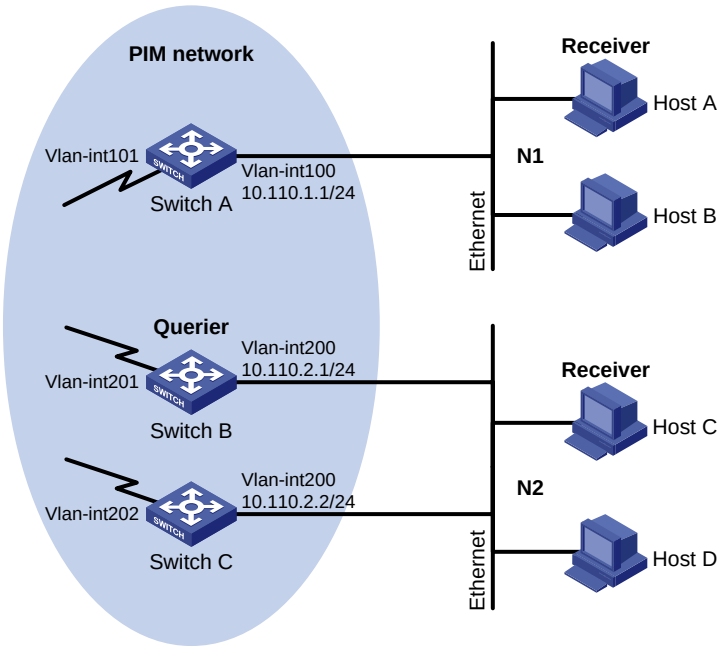
Basic IGMP functions configuration example

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.
- Switch A in the PIM network connects to N1, and both Switch B and Switch C connect to N2.
- Switch A connects to N1 through VLAN-interface 100, and to other devices in the PIM network through VLAN-interface 101.
- Switch B and Switch C connect to N2 through their respective VLAN-interface 200, and to other devices in the PIM network through VLAN-interface 201 and VLAN-interface 202 respectively.
- IGMPv2 is required between Switch A and N1. IGMPv2 is also required between the other two switches and N2. Switch B acts as the IGMP querier in N2 because it has a lower IP address.

Network diagram

Figure 35 Network diagram for basic IGMP functions configuration



Procedure

1. Configure the IP address and subnet mask of each interface as shown in Figure 35. The detailed configuration steps are omitted here.
2. Configure the OSPF protocol for interoperation on the PIM network. Ensure the network-layer interoperation on the PIM network and dynamic update of routing information among the switches through a unicast routing protocol. The detailed configuration steps are omitted here.
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. Verify the configuration

Use the **display igmp interface** command to view the IGMP configuration and operation status on each switch interface. For example:

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
```

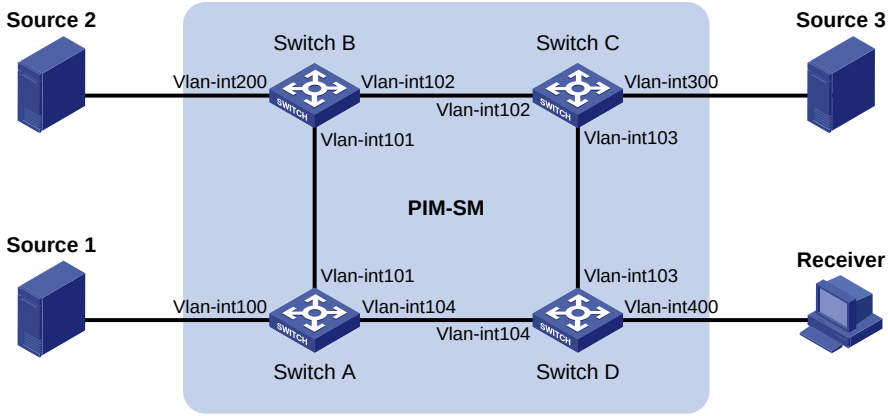
SSM mapping configuration example

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. 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. 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.

Network diagram

Figure 36 Network diagram for IGMP SSM mapping configuration



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

Procedure

1. Configure the IP address and subnet mask of each interface as shown in Figure 36. The detailed configuration steps are omitted here.
2. Configure OSPF for interoperability among the switches. Ensure the network-layer interoperation on the PIM-SM domain and dynamic update of routing information among the switches through a unicast routing protocol. The detailed configuration steps are omitted here.
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
```

The configuration on Switch B and Switch C is similar to that on Switch A.

4. Configure a C-BSR and a C-RP

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
```

The configuration on Switch A, Switch B and Switch C is similar to that on Switch D.

6. Configure IGMP SSM mappings

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
```

7. Verify the configuration

Use the **display igmp ssm-mapping** command to view the IGMP SSM mappings on the switch.

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 address: 232.1.1.1
Source list:
            133.133.1.1
            133.133.3.1
```

Use the **display igmp ssm-mapping group** command to view the multicast group information created based on the configured IGMP SSM mappings.

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
```

Use the **display pim routing-table** command to view the PIM routing table information on each switch.

Display the 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: -
```

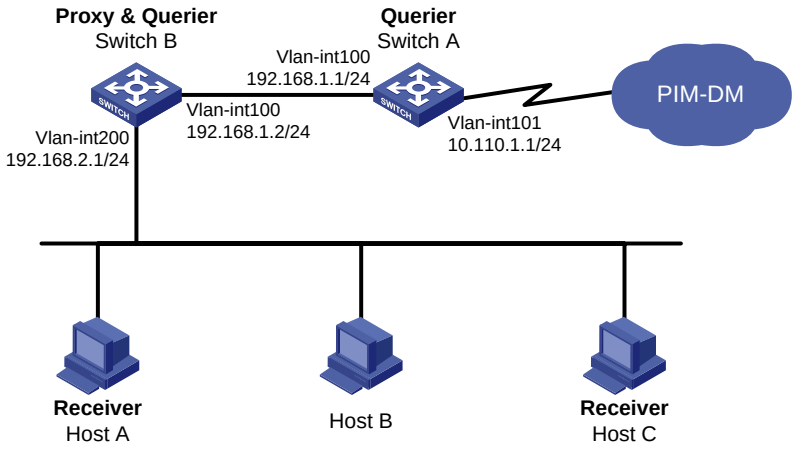
IGMP proxying configuration example

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.

Network diagram

Figure 37 Network diagram for IGMP Proxying configuration



Procedure

1. Configure IP addresses

Configure the IP address and subnet mask of each interface as shown in Figure 37. The detailed configuration steps are omitted here.

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
```

3. Verify the configuration

Use the **display igmp interface** command to view the IGMP configuration and operation information on an interface. For example

Display the IGMP configuration and operation 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
```

Use the **display igmp group** command to view the IGMP group information. For example,

Display the 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. Verify that the networking, interface connection, and IP address configuration are correct. Determine the interface information using **display igmp interface**. If the device has no 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 IP address configuration is incorrect.
2. Verify that multicast routing is enabled. Use **display current-configuration** to determine whether **multicast routing-enable** has been executed. If not, use **multicast routing-enable** in system view to enable IP multicast routing. In addition, verify that IGMP is enabled on the corresponding interfaces.
3. Determine the IGMP version on the interface. Use **display igmp interface** to determine whether the IGMP version on the interface is lower than that on the host.
4. Verify that no ACL rule has been configured to restrict the host from joining the multicast group G. Use **display current-configuration interface** to determine whether **igmp group-policy** has been executed. If the host cannot join the multicast group G, modify the ACL rule 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 IGMP version, 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. Check the IGMP configuration. Use **display current-configuration** to determine the IGMP configuration information on the interfaces.
2. Use **display igmp interface** on all routers on the same subnet to determine the IGMP-related timer settings. Be sure that the settings are consistent on all routers.
3. Use **display igmp interface** to determine whether all routers on the same subnet are running the same version of IGMP.

Configuring PIM

PIM provides IP multicast forwarding by leveraging static routes or unicast routing tables generated by any unicast routing protocol, such as RIP, OSPF, IS-IS, or BGP. Independent of the unicast routing protocols that are running on the switch, you can implement multicast routing as long as you create the corresponding multicast routing entries through unicast routes. PIM uses the RPF mechanism to implement multicast forwarding. When a multicast packet arrives on an interface of the switch, it undergoes an RPF verification. If the RPF verification succeeds, the device creates the corresponding routing entry and forwards the packet. If the RPF verification fails, the device discards the packet. For more information about RPF, see "Multicast routing and forwarding configuration."

Based on the implementation mechanism, PIM falls into the following modes:

- PIM-DM
- PIM-SM
- BIDIR-PIM
- PIM-SSM

To facilitate description, the term *PIM domain* in this document refers to a network that comprises PIM-capable routers.

Interface view mentioned in this chapter can be VLAN interface view or Layer 3 Ethernet interface view. Layer 3 Ethernet interfaces refer to Ethernet interfaces configured to operate in route mode. To switch the operating mode of an Ethernet port, see *Layer 2 - LAN Switching Configuration Guide*.

Implementing PIM-DM

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 following describes the basic implementation of PIM-DM:

- PIM-DM assumes that at least one multicast group member exists on each subnet of a network and multicast data is flooded to all nodes on the network. 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, and then data is flooded again down these branches and 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 (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 an 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).

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 process of flood-and-prune.

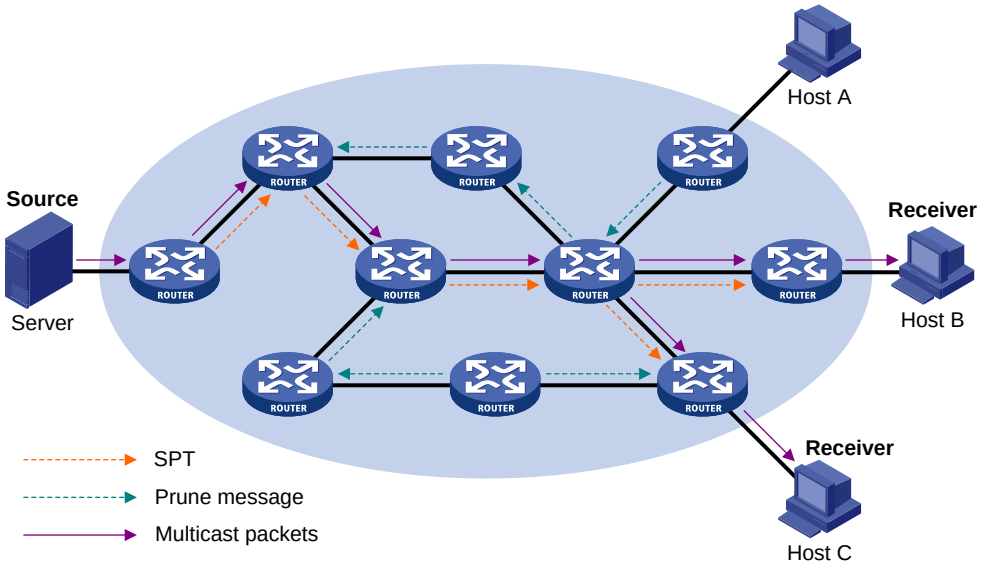
1. In a PIM-DM domain, when a multicast source S sends multicast data to multicast group G, the multicast packet is first flooded throughout the domain. The router first performs RPF check on the multicast packet. If the packet passes the RPF check, the router creates an (S, G) entry and forwards the 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. Nodes without downstream receivers are pruned. A router that has no downstream receivers 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 38, a router without any receiver attached to it (the router connected with Host A, for example) sends a prune message, and this prune process goes on until only necessary branches are left in the PIM-DM domain. These branches constitute the SPT.

Figure 38 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.

Pruning has a similar implementation in PIM-SM.

Graft

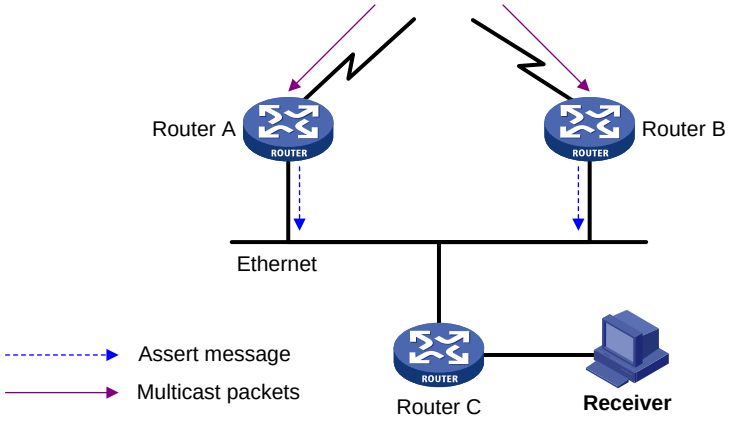
When a host attached to a pruned node joins a multicast group, to reduce the join latency, PIM-DM uses a graft mechanism to resume data forwarding to that branch.

1. The node that must receive multicast data sends a graft message toward its upstream node, as a request to join the SPT again.
2. Upon 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

The assert mechanism shuts off duplicate multicast flows onto the same multi-access network, where more than one multicast router exists, by electing a unique multicast forwarder on the multi-access network.

Figure 39 Assert mechanism



As shown in Figure 39, 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 local interface, receive a duplicate packet forwarded by the other. Upon detecting this condition, both routers send an assert message to all PIM routers (224.0.0.13) through the interface on which the packet was received.

The assert message contains the following information:

- Multicast source address (S)
- Multicast group address (G
- Preference and metric of the unicast 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 router with a higher unicast route preference to the source wins.
- If both routers have the same unicast route preference to the source, the router with a smaller metric to the source wins.
- If a tie occurs in route metric to the source, the router with a higher IP address of the local interface wins.

Implementing PIM-SM

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-sized 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 is to build and maintain RPTs. An RPT is rooted at a router in the PIM domain as the common node, or RP, through which the multicast data travels along the RPT and reaches the receivers.

- When a receiver is available for 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 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. Upon reaching the RP, the multicast packet is duplicated and delivered to the receivers along the RPT.

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 establishment
- 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.

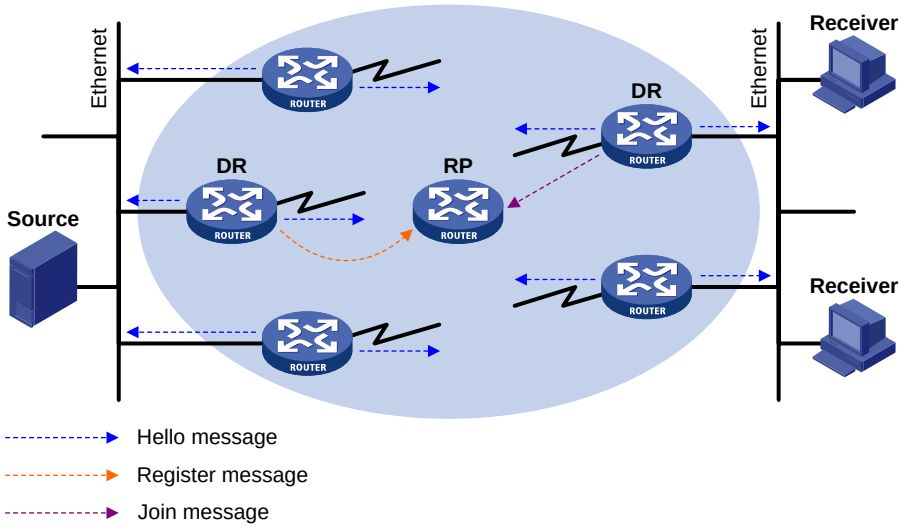
A DR must be elected in a multi-access network, whether this network connects to multicast sources or to receivers. The DR at the receiver side sends join messages to the RP; the DR at the multicast source side sends register messages to the RP.

A DR is elected on a multi-access subnet by means of comparison of the priorities and 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 *IP Multicast Configuration Guide*.

Figure 40 Figure DR election



As shown in Figure 40, the following describes the DR election process:

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. If a tie occurs 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

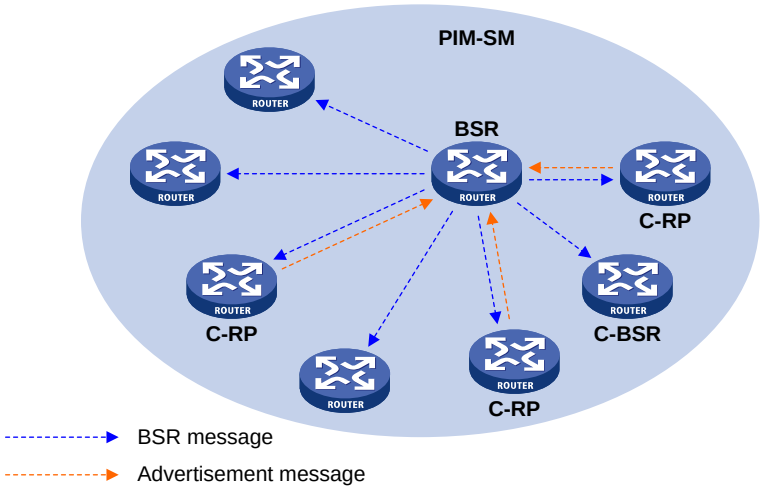
The RP is the core of a PIM-SM domain. For a small-sized, simple network, one RP is enough for forwarding information throughout the network, and you can statically specify the position of the RP on each router in the PIM-SM domain. In most cases, however, a PIM-SM network covers a wide area and a huge amount of multicast traffic must be forwarded through the RP. To lessen the RP burden and optimize the topological structure of the RPT, configure multiple C-RPs in a PIM-SM domain, among which an RP is dynamically elected through the bootstrap mechanism. Each elected RP serves a different multicast group range. For this purpose, you must configure a BSR. The BSR serves as the administrative core of the PIM-SM domain. A 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.

An RP can serve multiple multicast groups or all multicast groups. Only one RP can serve a given multicast group at a time.

A device can serve as a C-RP and a C-BSR at the same time.

As shown in Figure 41, each C-RP periodically sends its advertisement messages (C-RP-Adv messages) through unicast to the BSR. A C-RP-Adv message contains the address of the advertising C-RP and the multicast group range that it serves. The BSR collects these advertisement messages and chooses the appropriate C-RP information for each multicast group to form an RP-set, which is a database of mappings between multicast groups and RPs. The BSR then encapsulates the RP-set in the BSMs that it periodically originates and floods the bootstrap messages to the entire PIM-SM domain.

Figure 41 BSR and C-RPs



Based on the information in the RP-sets, all routers in the network can calculate the location of the corresponding RPs based on the following rules:

- The C-RP with the highest priority wins.
- If all the C-RPs have the same priority, their hash values are calculated through the hashing algorithm. The C-RP with the largest hash value wins.
- If all the C-RPs have the same priority and hash value, the C-RP with the highest IP address wins.

The hashing algorithm used for RP calculation is:

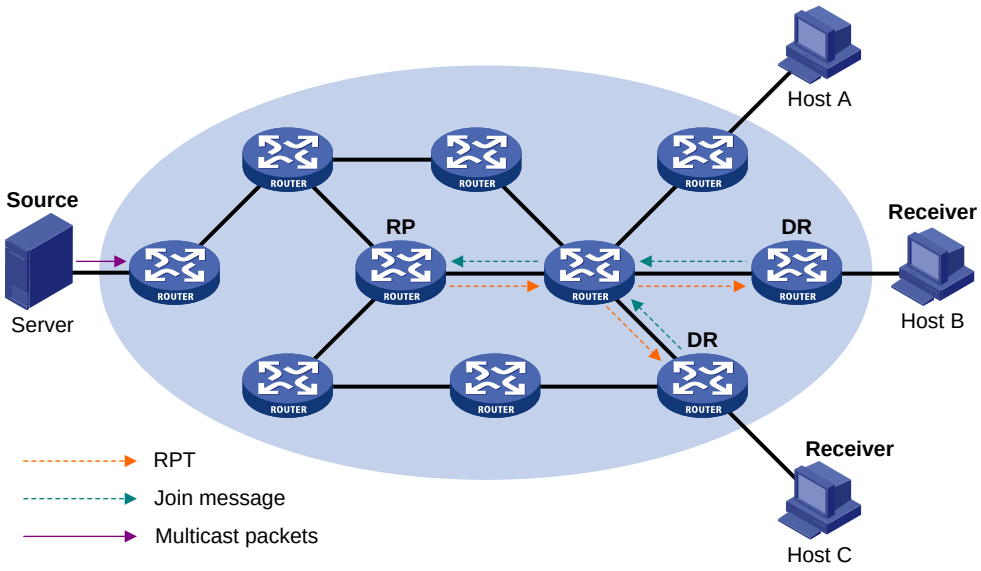
Value (G, M, C_i) = (1103515245 * ((1103515245 * (G & M) + 12345) XOR C_i) + 12345) mod 2^{31}

Table 8 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”
Mod	Modulo operator, which gives the remainder of an integer division

RPT building

Figure 42 RPT building in a PIM-SM domain



As shown in Figure 42, the following describes the process of building an RPT:

1. When a receiver joins multicast group G, it uses an IGMP message to inform the directly connected DR.
2. Upon 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 and the DRs are the leaves of the RPT.

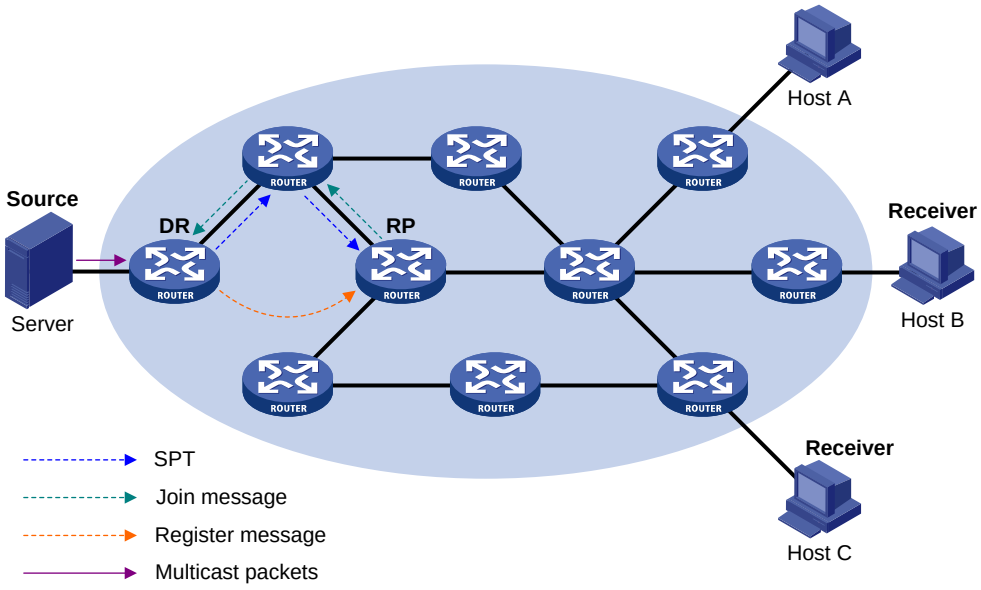
The multicast data addressed to the multicast group G flows through the RP, reaches the corresponding DR along the established RPT, and finally is delivered to the receiver.

When a receiver is no longer available for 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. Upon receiving the prune message, the upstream node deletes the interface connected with this downstream node from the outgoing interface list and determines whether it itself 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 is to inform the RP about the existence of the multicast source.

Figure 43 Multicast source registration



As shown in Figure 43, the following describes the process that how a multicast source registers with the RP:

1. When the multicast source S sends the first multicast packet to multicast group G, the DR directly connected with the multicast source, upon receiving the multicast packet, encapsulates the packet in a PIM register message and 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. 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 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, and 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.

The RP is configured to initiate an SPT switchover as described in this section. Otherwise, the DR at the 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 a PIM-SM domain, a multicast group corresponds to one RP and RPT. Before the SPT switchover occurs, the DR at the multicast source side encapsulates all multicast data destined to the multicast group in register messages and sends these messages to the RP. Upon 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.

This creates the following issues:

- The source-side DR and the RP must 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 to the RP, increasing the risk of failure.

To resolve these issues, PIM-SM allows an RP or the receiver-side DR to initiate an SPT switchover process. After receiving the first multicast packet, 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. The subsequent multicast data from the multicast source travels along the established SPT to the RP.

Upon receiving the first 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 multicast source. When the join message reaches the source-side DR, all the routers on the path have created the (S, G) entry in their forwarding table, and 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. Upon receiving this prune message, the RP sends a prune message toward the multicast source (suppose only one receiver exists) to implement the SPT switchover.
- Multicast data is directly sent from the source to the receivers along the SPT.

PIM-SM builds SPTs through SPT switchover more economically than PIM-DM does through the flood-and-prune mechanism.

Assert

PIM-SM uses an assert mechanism that is similar to what PIM-DM uses. For more information see “Assert.”

Impementing BIDIR-PIM

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 is introduced to address this 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 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.

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 that corresponds 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.

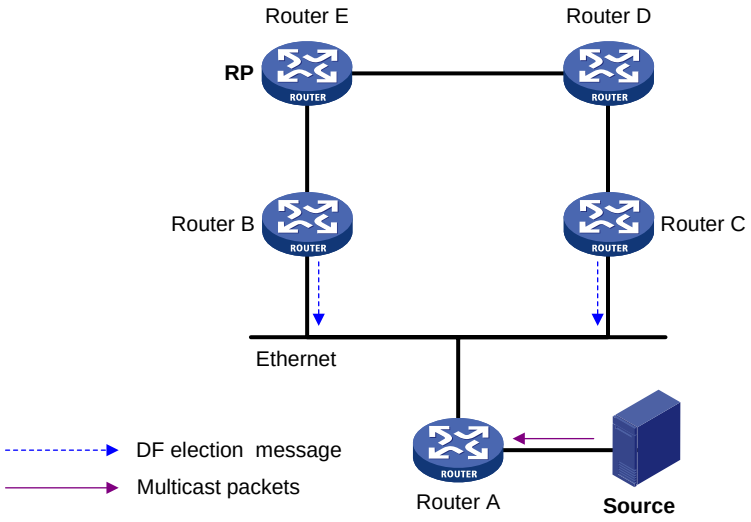
In BIDIR-PIM, an RPF interface is the interface pointing to an RP, and an RPF neighbor is the address of the next hop to the RP.

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.

DF election is not necessary for an RPL.

Figure 44 DF election



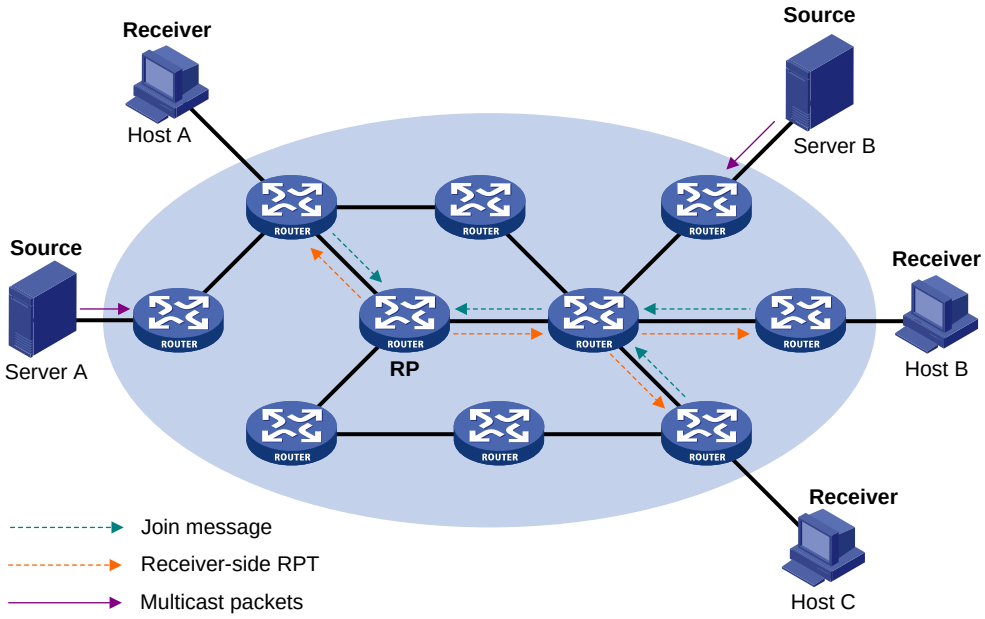
As shown in Figure 44, without the DF election mechanism, both Router B and Router C can receive multicast packets from Route A, and they might both forward the packets to downstream routers on the local subnet. As a result, the RP—Router E—receives duplicate multicast packets. With the DF election mechanism, 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 address, and the priority and metric of the unicast route, MBGP route, or multicast static route to the RP.
2. The router with a route of the highest priority becomes the DF.
3. If a tie occurs in the priority, the router with the route with the lowest metric wins the DF election.
4. If a tie occurs in the metric, the router with the highest IP address wins.

Bidirectional RPT building

A bidirectional RPT comprises receiver-side RPT and 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 sources as leaves. The processes for building these two parts are different.

Figure 45 RPT building at the receiver side

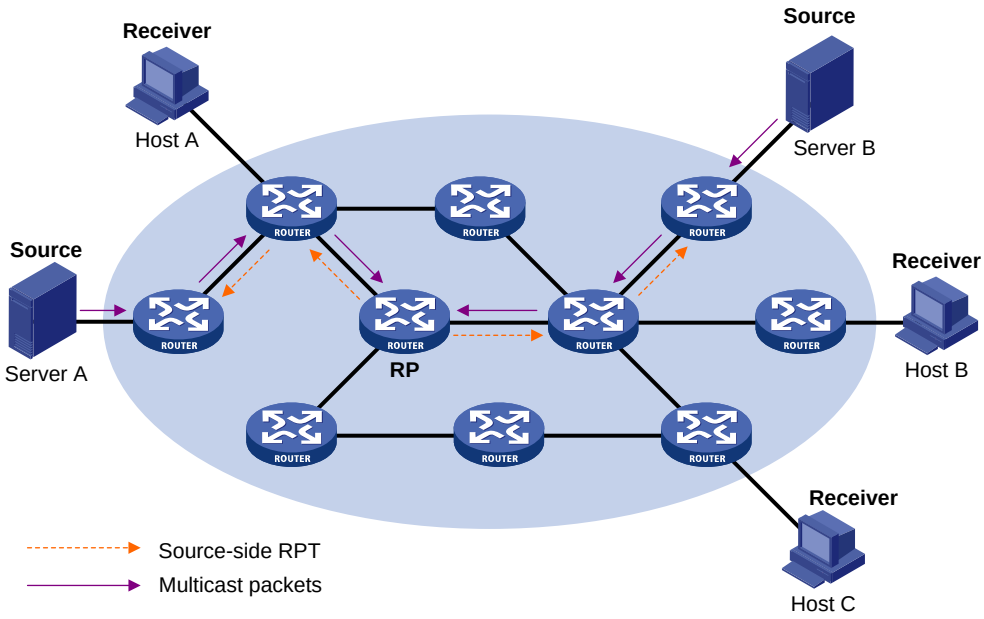


As shown in Figure 45, the process for building a receiver-side RPT is similar to that for building an RPT in PIM-SM:

1. When a receiver joins multicast group G, it uses an IGMP message to inform the directly connected router.
2. Upon 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. Upon 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 multicast group. If not, the router continues to forward the prune message to its upstream router.

Figure 46 RPT building at the multicast source side



As shown in Figure 46, the process of building a source-side RPT is relatively simple. First, when a multicast source sends multicast packets to multicast group G, the DF in each network segment unconditionally forwards the packets to the RP.

Then, the routers along the path from the sources 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.

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 are directly forwarded by the node to the receiver, instead of by the RP.

Administrative scoping

Division of PIM-SM domains

Typically, a PIM-SM/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 a "non-scoped BSR mechanism."

To implement refined management, you can divide a PIM-SM/BIDIR-PIM domain into one global-scope zone and multiple administratively scoped zones (admin-scope zones). This is called an "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. ZBRs form the boundary of the admin-scope zone. Each admin-scope zone maintains one BSR, which serves 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 that different admin-scope zones

serve 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 serves the multicast groups that do not belong to any admin-scope zone.

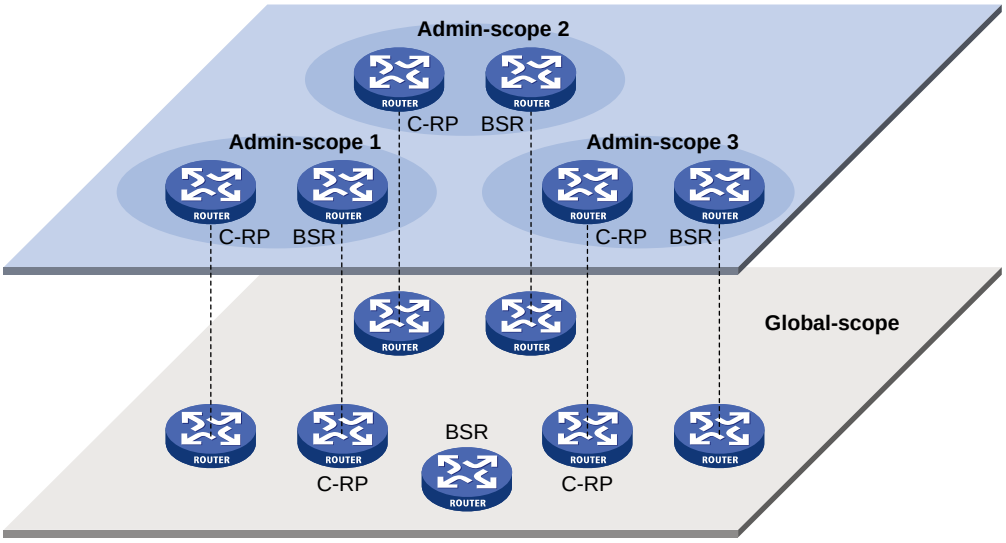
Relationship between admin-scope zones and the global scope zone

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. Namely, BSR election and RP election are implemented independently within each admin-scope zone. Each admin-scope zone has its own boundary. The multicast information cannot cross this border in either direction. A better understanding of the global-scope zone and admin-scope zones should be based on geographical space and group address range.

Geographical space

Admin-scope zones are logical zones specific to particular multicast groups. The multicast packets of these multicast groups are confined within the local admin-scope zone and cannot cross the boundary of the zone.

Figure 47 Relationship between admin-scope zones and the global-scope zone in geographic space

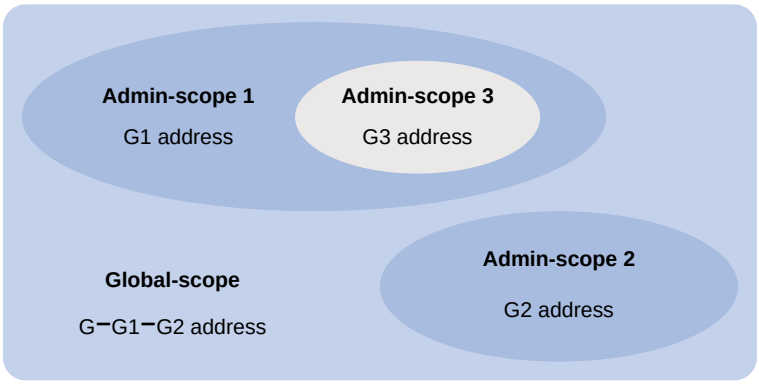


As shown in Figure 47, for multicast groups in the same address range, admin-scope zones must be geographically separated from one another. Namely, a router must not serve different admin-scope zones. Different admin-scope zones contain different routers, whereas the global-scope zone covers all routers in the PIM-SM/BIDIR-PIM domain. Multicast packets that do not belong to any admin-scope zones can be transmitted in the entire PIM-SM/BIDIR-PIM domain.

Multicast group address ranges

Each admin-scope zone serves specific multicast groups. Usually, these addresses have no intersections; however, they can overlap one another.

Figure 48 Relationship between admin-scope zones and the global-scope zone in group address ranges



In Figure 48, the group address ranges of admin-scope 1 and 2 have no intersection, whereas the group address range of admin-scope 3 is a subset of the address range of admin-scope 1. The group address range of the global-scope zone—G-G1-G2—covers all the group addresses other than those of all the admin-scope zones. A supplementary relationship exists between the global-scope zone and all the admin-scope zones in terms of group address ranges.

Implementing PIM-SSM

The SSM model and the 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.

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 the 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. As a result, no RP or RPT is required, no source registration process exists, and no need exists to use MSDP for discovering sources in other PIM domains.

The working mechanism of PIM-SSM can be 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."

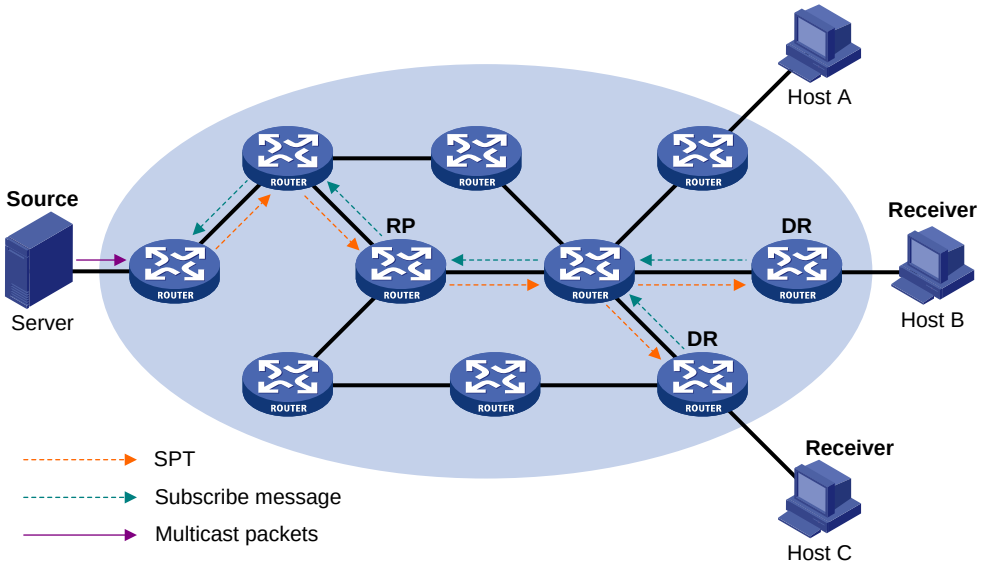
DR election

PIM-SSM uses the same DR election mechanism as in PIM-SM. See "DR election."

Construction of SPT

Whether to build an RPT for PIM-SM or an SPT for PIM-SSM depends on whether the multicast group the receiver joins falls in the SSM group range (SSM group range reserved by IANA is 232.0.0.0/8).

Figure 49 SPT building in PIM-SSM



As shown in Figure 49, 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 in the SSM group range:

- If so, 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 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 not, the DR follows the PIM-SM process. The DR must send a (*, G) join message to the RP and start a multicast source registration process.

In PIM-SSM, the term *channel* refers to a multicast group, and the term *channel subscription* refers to a join message.

Multi-Instance PIM

A multicast router that is running multiple instances maintains an independent set of PIM neighbor table, multicast routing table, BSR information, and RP-set information for each instance.

Upon receiving a multicast data packet, the multicast router determines the VPN instance that the data packet belongs to, and then forwards the packet according to the multicast routing table of that VPN instance or creates a multicast routing table entry for that VPN instance.

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

Prerequisites

Before configuring 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 deploying a PIM-DM domain, enable PIM-DM on all non-border interfaces of the routers.

Enabling PIM-DM globally for the public network

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enable IP multicast routing.	**multicast routing-enable**	Required. Disable by default.
3. Enter interface view.	**interface** *interface-type interface-number*	—
4. Enable PIM-DM.	**pim dm**	Required. Defaults to disabled.

Enabling PIM-DM in a VPN instance

All the interfaces in the same VPN instance on the same device must work in the same PIM mode. PIM-DM does not work with multicast groups in the SSM group range.

To do...	Use the command...	Description
1. Enter system view.	**system-view**	—
2. Create a VPN instance and enter VPN instance view.	**ip vpn-instance** *vpn-instance-name*	—
3. Configure a route-distinguisher 4. (RD) for the VPN instance.	**route-distinguisher** *route-distinguisher*	Required Not configured by default
5. Enable IP multicast routing.	**multicast routing-enable**	Required. Defaults to disabled.

To do...	Use the command...	Description
6. Enter interface view.	**interface** *interface-type interface-number*	—
7. Associate the current interface with the VPN instance.	**ip binding vpn-instance** *vpn-instance-name*	Required. No VPN instance is associated with an interface by default.
8. Enable PIM-DM.	**pim dm**	Required. Defaults to disabled.

For more information about **ip vpn-instance**, **route-distinguisher** and **ip binding vpn-instance**, see *MPLS Command Reference*.

For more information about **multicast routing-enable**, 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
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 an interval for sending such messages.

A router might receive multiple state-refresh messages within a short time, of which some 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 the 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, you must configure an appropriate TTL value based on the network size.

To configure the state-refresh parameters, complete the following configurations on all routers in the PIM domain.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—

To do...	Use the command...	Remarks
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure the interval between state-refresh messages.	**state-refresh-interval** *interval*	Optional. Defaults to 60 seconds.
4. Configure the time to wait before receiving a new state-refresh message.	**state-refresh-rate-limit** *interval*	Optional. Defaults to 30 seconds.
5. Configure the TTL value of state-refresh messages.	**state-refresh-ttl** *ttl-value*	Optional. Defaults to 255.

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 (graft retry period) until it receives a graft-ack messages from the upstream router.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure graft retry period.	**pim timer graft-retry** *interval*	Optional. Defaults to 3 seconds.

Configuring PIM-SM

Prerequisites

Before configuring 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 defining the range of multicast groups to be served by the static RP
- Determine the C-RP priority and the ACL defining the range of multicast groups to be served by each C-RP
- Determine the legal C-RP address range and the ACL defining the range of multicast groups to be served
- 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 for register message filtering
- Determine the register suppression time
- Determine the register probe time
- Determine the ACL, and sequencing rule for disabling an SPT switchover.

Enabling PIM-SM

When PIM-SM is enabled, a router sends hello messages periodically to discover PIM neighbors and processes messages from the PIM neighbors. When you deploy a PIM-SM domain, enable PIM-SM on all non-border interfaces of the routers.

Enabling PIM-SM globally for the public network

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enable IP multicast routing.	**multicast routing-enable**	Required. Defaults to disabled.
3. Enter interface view.	**interface** *interface-type interface-number*	—
4. Enable PIM-SM.	**pim sm**	Required Defaults to disabled.

Enabling PIM-SM in a VPN instance

All the interfaces in the same VPN instance on the same router must work in the same PIM mode.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Create a VPN instance and enter VPN instance view.	**ip vpn-instance** *vpn-instance-name*	—
3. Configure a route-distinguisher 4. (RD) for the VPN instance.	**route-distinguisher** *route-distinguisher*	Required Not configured by default
5. Enable IP multicast routing.	**multicast routing-enable**	Required Defaults to disabled.
6. Enter interface view.	**interface** *interface-type interface-number*	—
7. Associate the current interface with the VPN instance.	**ip binding vpn-instance** *vpn-instance-name*	Required. No VPN instance is associated with an interface by default.
8. Enable PIM-SM.	**pim sm**	Required. Defaults to disabled.

For more information about **ip vpn-instance**, **route-distinguisher** and **ip binding vpn-instance**, see *MPLS Command Reference*.

For more information about **multicast routing-enable**, 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 means for the dynamic RP election mechanism to enhance the robustness and operational manageability of a multicast network.

Configuring a static RP

If only one dynamic RP exists in a network, configuring a static RP can avoid communication interruption due to single-point failures and avoid frequent message exchange between C-RPs and the BSR.

Perform this configuration on all the routers in the PIM-SM domain.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure a static RP for PIM-SM.	**static-rp** *rp-address* [*acl-number*] [**preferred**]	Required. No static RP by default.

To enable a static RP to work normally, you must perform this configuration on all the routers in the PIM-SM domain and specify the same RP address.

Configuring a C-RP

In a PIM-SM domain, you can configure routers that will 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. 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 be served 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 configuring a C-RP, ensure a relatively large bandwidth between this C-RP and the other devices in the PIM-SM domain.

An RP can serve multiple multicast groups or all multicast groups. Only one RP can forward multicast traffic for a multicast group at a moment.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—

To do...	Use the command...	Remarks
3. Configure an interface to be a C-RP for PIM-SM.	**c-rp** *interface-type interface-number* [**group-policy** *acl-number* | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] *	Required. No C-RP is configured by default.
4. Configure a legal C-RP address range and the range of multicast groups to be served.	**crp-policy** *acl-number*	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, respectively. With auto-RP enabled on a device, the device can receive these types of messages and record the RP information carried in such messages.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Enable auto-RP.	**auto-rp enable**	Required. Defaults to disabled.

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 obtains 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. Upon 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure the C-RP-Adv interval.	**c-rp advertisement-interval** *interval*	Optional. Defaults to 60 seconds.
4. Configure C-RP timeout time.	**c-rp holdtime** *interval*	Optional. Defaults to 150 seconds.

Configuring a BSR

A PIM-SM domain can have only one BSR, but must have at least one C-BSR. You can configure any router 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

Configure C-BSRs on routers in the backbone network. When configuring a router as a C-BSR, be sure to specify a PIM-SM-enabled interface on the router. The following summarizes the BSR election process:

- 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.
- 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 occurs 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, to prevent a maliciously configured host from masquerading as a BSR. Make the same configuration on all routers in the PIM-SM 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 verifications and RPF verifications on bootstrap messages and discard unwanted messages.
- If an attacker controls a router in the network or if an illegal router is present in the network, the attacker can configure this router as a C-BSR and make it win the 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 entire 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 partially protect the security of BSRs in a network. However, if an attacker controls a legal BSR, the issue still occurs.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM viewor VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure an interface as a C-BSR.	**c-bsr** *interface-type interface-number* [*hash-length* [*priority*]]	Required. 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.

Because a large amount of information needs to be exchanged between a BSR and the other devices in the PIM-SM domain, provide a relatively large bandwidth between the C-BSRs and the other devices in the PIM-SM domain.

For C-BSRs interconnected using a GRE tunnel, configure multicast static routes to make sure that the next hop to a C-BSR is a GRE interface. For more information about multicast static routes, see *IP Multicast Configuration Guide*.

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 can become a PIM domain border.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure a PIM domain border.	**pim bsr-boundary**	Required. 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.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure the hash mask length.	**c-bsr hash-length** *hash-length*	Optional. 30 by default.
4. Configure the C-BSR priority.	**c-bsr priority** *priority*	Optional. By default, the C-BSR priority is 64.

Hash mask length and C-BSR priority

You can configure these parameters at three levels:

- Global configuration level
- Global scope zone level
- Admin-scope zone level

Parameter values configured at the global scope zone level or admin-scope zone level have preference over the global configuration level values, and default to the global value level.

Configuring C-BSR timers

The BSR election winner multicasts its own IP address and RP-Set information through bootstrap messages within the entire zone it serves. 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 the BSR state times out and no bootstrap message is received from the BSR, a new BSR election process is triggered among the C-BSRs.

Configure C-BSR timers on C-BSR routers.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure the BS period.	**c-bsr interval** *interval*	Optional. For the default value, see the note under this table.
4. Configure the BS timeout.	**c-bsr holdtime** *interval*	Optional. For the default value, see the note under this table.

BS period and timeout settings

Make sure that the BS period value is smaller than the BS timeout value.

The BS period defaults to the value 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 timeout setting defaults to the value determined by the formula:

"BS timeout = BS period × 2 + 10". The default BS period is 60 seconds, so the default BS timeout = 60 × 2 + 10 = 130 (seconds)

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).

- Upon 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 upon 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.

The function of BSM semantic fragmentation is enabled by default. Devices not supporting this function might deem a fragment as an entire message, learning 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 do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Disable the BSM semantic fragmentation function.	**undo bsm-fragment enable**	Required. By default, the BSM semantic fragmentation function is enabled.

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.

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 serves a specific multicast group range. The global-scope zone also maintains a BSR, which serves all the remaining multicast groups.

Enabling administrative scoping

Before configuring an admin-scope zone, enable administrative scoping. Configure administrative scoping on routers that can become a C-BSR and ZBR.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Enable administrative scoping.	**c-bsr admin-scope**	Required. Defaults to disabled.

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 serves 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.

Configure an admin-scope zone boundary on routers that can become a ZBR. Use the *group-address* { *mask* | *mask-length* } parameter of **multicast boundary** to specify the multicast groups an admin-scope zone serves, in the range of 239.0.0.0/8.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—

To do…	Use the command…	Remarks
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure a multicast forwarding boundary.	**multicast boundary** *group-address* { *mask* | *mask-length* }	Required. By default, no multicast forwarding boundary is configured.

For more information about the **multicast boundary** command, see *IP Multicast Command Reference*.

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 on the routers that work as C-BSRs in admin-scope zones.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure a C-BSR for an admin-scope zone.	**c-bsr group** *group-address* { *mask* | *mask-length* } [**hash-length** *hash-length* | **priority** *priority*] *	Required. No C-BSRs are configured for an admin-scope zone by default.

Use the *group-address* { *mask* | *mask-length* } parameter of **c-bsr group** to specify the multicast groups the C-BSR serves, in the range of 239.0.0.0/8.

Configure C-BSRs for the global-scope zone on the routers that work as C-BSRs in the global-scope zone.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure a C-BSR for the global-scope zone.	**c-bsr global** [**hash-length** *hash-length* | **priority** *priority*] *	Required. No C-BSRs are configured for the global-scope zone by default.

Hash mask length and C-BSR priority

You can configure these parameters at three levels:

- Global configuration level
- Global scope zone level
- Admin-scope zone level

Parameter values configured at the global scope zone level or admin-scope zone level have preference over the global configuration level values, and default to the global value level.

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 serve specific multicast groups. If the filtering rule denies an (S, G) entry, or the filtering rule does not define the action for this entry, the RP sends 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, HP does not recommend using this method of checksum calculation.

When receivers stop receiving multicast data addressed to a certain multicast group through the RP (the RP stops serving the receivers of that multicast group), or when the RP formally starts receiving register messages with multicast data encapsulated from the multicast source, 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. When 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure a filtering rule for register messages.	**register-policy** *acl-number*	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** *interval*	Optional. Defaults to 60 seconds.
6. Configure the register probe time.	**probe-interval** *interval*	Optional Defaults to 5 seconds.

Disabling SPT switchover

If an A5820X or A5800 switch acts as an RP or the receiver-side DR, it initiates an STP switchover process (by default) upon receiving the first multicast packet along the RPT. You can disable the switchover from RPT to SPT.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Disable the SPT switchover.	**spt-switch-threshold infinity** [**group-policy** *acl-number* [**order** *order-value*]]	Optional. By default, the device switches to the SPT immediately after it receives the first multicast packet.

A5820X & A5800 Switch Series

After a multicast forwarding entry is created, subsequent multicast data is not encapsulated in register messages before being forwarded, even if a register outgoing interface is available. To avoid forwarding failure, do not use **spt-switch-threshold infinity** on a switch that might become an RP (a static RP or a C-RP).

Configuring BIDIR-PIM

Prerequisites

Before configuring BIDIR-PIM, complete the following tasks:

- Configure a 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 that defines the range of the multicast groups to be served by the static RP
- Determine the C-RP priority and the ACL that defines the range of multicast groups to be served by each C-RP
- Determine the legal C-RP address range and the ACL that defines the range of multicast groups to be served
- 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.

Enabling PIM-SM globally for the public network

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enable IP multicast routing.	**multicast routing-enable**	Required. Defaults to disabled.
3. Enter interface view.	**interface** *interface-type interface-number*	—
4. Enable PIM-SM.	**pim sm**	Required. Defaults to disabled.

Enabling PIM-SM in a VPN instance

On a router, all interfaces in the same VPN instance must work in the same PIM mode.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Create a VPN instance and enter VPN instance view.	**ip vpn-instance** *vpn-instance-name*	—
3. Configure an RD for the VPN instance.	**route-distinguisher** *route-distinguisher*	Required. Not configured by default.
4. Enable IP multicast routing.	**multicast routing-enable**	Required. Defaults to disabled.
5. Enter interface view.	**interface** *interface-type interface-number*	—
6. Bind the interface with the VPN instance.	**ip binding vpn-instance** *vpn-instance-name*	Required. By default, an interface belongs to the public network, and it not bound with any VPN instance.
7. Enable PIM-SM.	**pim sm**	Required. Defaults to disabled.

For more information about **ip vpn-instance**, **route-distinguisher**, and **ip binding vpn-instance**, see *MPLS Command Reference*.

For more information about **multicast routing-enable**, see *IP Multicast Command Reference*.

Enabling BIDIR-PIM

Enable BIDIR-PM on all routers in the BIDIR-PIM domain.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—

To do...	Use the command...	Remarks
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Enable BIDIR-PIM.	**bidir-pim enable**	Required. Defaults to disabled.

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 means for the dynamic RP election mechanism to enhance the robustness and operation manageability of a multicast network.

CAUTION:

In a PIM network, if both PIM-SM and BIDIR-PIM are enabled, do not configure the same RP to serve PIM-SM and BIDIR-PIM simultaneously to avoid PIM routing table errors.

Configuring a static RP

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, specify a virtual IP address, like 10.1.1.100/24, for the static RP. As a result, the link becomes an RPL. If only one dynamic RP exists in a network, configuring a static RP can avoid communication interruption due to single-point failures and avoid frequent message exchange between C-RPs and the BSR.

Configure static RP on all routers in the BIDIR-PIM domain and in the PIM-SM domain and specify the same RP address.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure a static RP for BIDIR-PIM.	**static-rp** *rp-address* [*acl-number*] [**preferred**] **bidir**	Required. 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 be served 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 configuring a C-RP, ensure a relatively large bandwidth between this C-RP and the other devices in the BIDIR-PIM domain.

An RP can serve multiple multicast groups or all multicast groups. Only one RP can forward multicast traffic for a multicast group at a moment.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure an interface to be a C-RP for BIDIR-PIM.	**c-rp** *interface-type interface-number* [**group-policy** *acl-number* | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] * **bidir**	Required. 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 respectively. 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Enable auto-RP.	**auto-rp enable**	Required. Defaults to disabled.

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. Upon 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.

Configure C-RP timers on all C-RP routers.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure the C-RP-Adv interval.	**c-rp advertisement-interval** *interval*	Optional. Defaults to 60 seconds.
4. Configure C-RP timeout time.	**c-rp holdtime** *interval*	Optional. Defaults to 150 seconds.

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. You can configure any router 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 configuring a router as a C-BSR, be sure to specify a BIDIR-PIM-enabled interface on the router. The following summarizes the BSR election process:

- 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.
- 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 occurs 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, 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, a BSR can be protected against attacks from external hosts after you enable 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. However, if a legal BSR is controlled by an attacker, the mentioned problem will still occur.

To do…	Use the command…	Remarks
1. Enter system view	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure an interface as a C-BSR.	**c-bsr** *interface-type interface-number* [*hash-length* [*priority*]]	Required 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.

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.

For C-BSRs interconnected through a GRE tunnel, multicast static routes need to be configured to ensure that the next hop to a C-BSR is a Tunnel interface. For more information about multicast static routes, see the chapter "Multicast routing and forwarding configuration."

Configuring a 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 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 BIDIR-PIM domains. Bootstrap messages cannot cross a domain border in either direction.

Configure PIM domain border on routers that are intended to form the PIM domain border.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure a PIM domain border.	**pim bsr-boundary**	Required. By default, no 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 that corresponds to specific multicast groups.

Configure global C-BSR parameters on C-BSR routers.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure the hash mask length.	**c-bsr hash-length** *hash-length*	Optional. Defaults to 30.
4. Configure the C-BSR priority.	**c-bsr priority** *priority*	Optional Defaults to 64.

Hash mask length and C-BSR priority

You can configure these parameters at three levels:

- Global configuration level
- Global scope zone level
- Admin-scope zone level

Parameter values configured at the global scope zone level or admin-scope zone level have preference over the global configuration level values, and default to the global value level.

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."

Configuring C-BSR timers

The BSR election winner multicasts its own IP address and RP-Set information through bootstrap messages within the entire zone it serves. 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 the BSR state times out and no bootstrap message is received from the BSR, a new BSR election process is triggered among the C-BSRs.

Configure C-BSR timers on C-BSR routers. Make sure that the BS period value is smaller than the BS timeout value.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure the BS period.	**c-bsr interval** *interval*	Optional. For the default value, see the note under this table.
4. Configure the BS timeout.	**c-bsr holdtime** *interval*	Optional. For the default value, see the note under this table.

BS period and timeout settings

Make sure that the BS period value is smaller than the BS timeout value.

The BS period defaults to the value 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 timeout setting defaults to the value determined by the formula:

"BS timeout = BS period × 2 + 10". The default BS period is 60 seconds, so the default BS timeout = 60 × 2 + 10 = 130 (seconds)

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 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).

- Upon 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 upon 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.

The function of BSM semantic fragmentation is enabled by default. Devices not supporting this function might deem a fragment as an entire message, 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.

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.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Disable the BSM semantic fragmentation function.	**undo bsm-fragment enable**	Required. 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 serves a specific multicast group range. The global-scope zone also maintains a BSR, which serves all the rest multicast groups.

Enabling administrative scoping

Before configuring an admin-scope zone, enable administrative scoping. Enable administrative scoping on routers that can become a C-BSR and ZBR.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Enable administrative scoping.	**c-bsr admin-scope**	Required. Defaults to disabled.

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 serves 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.

Configure an admin-scope zone boundary on routers that can become a ZBR.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—

To do…	Use the command…	Remarks
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure a multicast forwarding boundary.	**multicast boundary** *group-address* { *mask* | *mask-length* }	Required. By default, no multicast forwarding boundary is configured.

Use the *group-address* { *mask* | *mask-length* } parameter of **multicast boundary** to specify the multicast groups that an admin-scope zone serves, in the range of 239.0.0.0/8. For more information about **multicast boundary**, see *IP Multicast Command Reference*.

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 that corresponds to the specific multicast group.

Configure C-BSRs for each admin-scope zone on the routers that work as C-BSRs in admin-scope zones.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure a C-BSR for an admin-scope zone.	**c-bsr group** *group-address* { *mask* | *mask-length* } [**hash-length** *hash-length* | **priority** *priority*] *	Required. No C-BSRs are configured for an admin-scope zone by default.

Use the *group-address* { *mask* | *mask-length* } parameter of **c-bsr group** to specify the multicast groups the C-BSR serves, in the range of 239.0.0.0/8.

Configure C-BSRs for the global-scope zoneon the routers that work as C-BSRs in the global-scope zone.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure a C-BSR for the global-scope zone.	**c-bsr global** [**hash-length** *hash-length* | **priority** *priority*] *	Required. No C-BSRs are configured for the global-scope zone by default.

Hash mask length and C-BSR priority

You can configure these parameters at three levels:

- Global configuration level
- Global scope zone level
- Admin-scope zone level

Parameter values configured at the global scope zone level or admin-scope zone level have preference over the global configuration level values, and default to the global value level.

For configuration of global C-BSR parameters, see "Configuring global C-BSR parameters."

Configuring PIM-SSM

The PIM-SSM model needs the support of IGMPv3. Be sure to enable IGMPv3 on PIM routers with multicast receivers. All the interfaces in the same VPN instance on the same device must work in the same PIM mode.

Prerequisites

Before configuring 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 SSM model is implemented based on some subsets of PIM-SM. Therefore, a router is PIM-SSM capable after you enable PIM-SM on it.

When you deploy a PIM-SM domain, HP recommends you to enable PIM-SM on non-border interfaces of the routers.

Enabling PIM-SM globally for the public network

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enable IP multicast routing.	**multicast routing-enable**	Required. Defaults to disabled.
3. Enter interface view.	**interface** *interface-type interface-number*	—
4. Enable PIM-SM.	**pim sm**	Required. Defaults to disabled.

Enabling PIM-SM in a VPN instance

To do...	Use the command...	Description
1. Enter system view.	**system-view**	—
2. Create a VPN instance and enter VPN instance view.	**ip vpn-instance** *vpn-instance-name*	—
3. Configure a route-distinguisher 4. (RD) for the VPN instance.	**route-distinguisher** *route-distinguisher*	Required. No RD is configured by default.
5. Enable IP multicast routing.	**multicast routing-enable**	Required. Defaults to disabled.

To do...	Use the command...	Description
6. Enter interface view.	**interface** *interface-type interface-number*	—
7. Associate the current interface with the VPN instance.	**ip binding vpn-instance** *vpn-instance-name*	Required. No VPN instance is associated with an interface by default.
8. Enable PIM-SM.	**pim sm**	Required. Defaults to disabled.

For more information about **ip vpn-instance**, **route-distinguisher** and **ip binding vpn-instance**, see *MPLS Command Reference*. For more information about **multicast routing-enable**, see *IP Multicast Command Reference*.

Configuring the SSM group range

Whether the information from a multicast source is delivered to the receivers based on the PIM-SSM model or the PIM-SM model depends on whether the group address in the (S, G) channel subscribed by the receivers falls in the SSM group range. All PIM-SM-enabled interfaces assume that multicast groups within this address range are using the PIM-SSM model.

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.

Perform the following configuration on all routers in the PIM-SM domain.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure the SSM group range.	**ssm-policy** *acl-number*	Optional. 232.0.0.0/8 by default.

Configuring PIM common features

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

If the same function or parameter is configured in both PIM view and interface view, the configuration made in interface view has preference over the configuration made in PIM view, regardless of the configuration sequence.

Prerequisites

Before you configuring 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 for filtering multicast data.
- Determine the ACL 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.

Configuring a multicast data filter

In both a PIM-DM domain and a PIM-SM domain, routers can examine passing-by multicast data based on the configured filtering rules and determine whether to continue forwarding the multicast data. PIM routers can act as multicast data filters. These filters can help implement traffic control and can control the information available to downstream receivers to enhance data security.

A shorter distance from the filter to the multicast source typically 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure a multicast group filter.	**source-policy** *acl-number*	Required. 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, and to guard against PIM message attacks.

With the hello message filter configured, if hello messages of an existing PIM neighbor fail to pass the filter, the PIM neighbor is removed automatically when it times out.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure a hello message filter.	**pim neighbor-policy** *acl-number*	Required. No hello message filter by default.

Configuring PIM hello options

In both a PIM-DM domain and a PIM-SM domain, the hello messages sent among routers contain the following 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 (namely, 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 will take 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 causes the upstream routers to delay the processing of 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 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 fails to explicitly track which downstream routers have joined.

Configuring hello options globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—

To do...	Use the command...	Remarks
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
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. Defaults to 105 seconds.
5. Configure the prune message delay time (LAN-delay).	**hello-option lan-delay** *interval*	Optional. 500 milliseconds by default.
6. Configure the prune override interval.	**hello-option override-interval** *interval*	Optional. 2,500 milliseconds by default.
7. Disable join suppression.	**hello-option neighbor-tracking**	Required. Enabled by default.

Configuring hello optionx on an interface

To do...	Use the command...	Remarks
8. Enter system view.	**system-view**	—
9. Enter interface view.	**interface** *interface-type interface-number*	—
10. Configure the priority for DR election.	**pim hello-option dr-priority** *priority*	Optional. 1 by default.
11. Configure PIM neighbor timeout time.	**pim hello-option holdtime** *interval*	Optional. Defaults to 105 seconds.
12. Configure the prune message delay time (LAN-delay).	**pim hello-option lan-delay** *interval*	Optional. 500 milliseconds by default.
13. Configure the prune override interval.	**pim hello-option override-interval** *interval*	Optional. 2,500 milliseconds by default.
14. Disable join suppression.	**pim hello-option neighbor-tracking**	Required. Enabled by default.
15. Configure the interface to reject hello messages without a generation ID.	**pim require-genid**	Required. By default, hello messages without Generation_ID are accepted.

Configuring the prune delay

If a downstream router does not support the prune override interval field, configure a prune delay interval on the upstream router so that it will not perform the prune action immediately after receiving the prune message. Instead, it maintains the current forwarding state for the prune delay interval. In this period, if the upstream router receives a join message from the downstream router, it cancels the prune action.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—

To do...	Use the command...	Remarks
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure the prune delay interval.	**prune delay** *interval*	Optional. 3 seconds by default.

Configuring PIM common timers

PIM routers discover PIM neighbors and maintain PIM neighboring relationships with other routers by periodically sending out hello messages.

Upon 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.

Configuring PIM common timers globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure the hello interval.	**timer hello** *interval*	Optional. Defaults to 30 seconds.
4. Configure the join/prune interval.	**timer join-prune** *interval*	Optional. Defaults to 60 seconds.
5. Configure the join/prune timeout time.	**holdtime join-prune** *interval*	Optional. Defaults to 210 seconds.
6. Configure assert timeout time.	**holdtime assert** *interval*	Optional. Defaults to 180 seconds.
7. Configure the multicast source lifetime.	**source-lifetime** *interval*	Optional. Defaults to 210 seconds.

Configuring PIM common timers on an interface

If there are no special networking requirements, HP recommends using the default settings.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure the hello interval.	**pim timer hello** *interval*	Optional. Defaults to 30 seconds.
4. Configure the maximum delay between hello messages.	**pim triggered-hello-delay** *interval*	Optional. Defaults to 5 seconds.
5. Configure the join/prune interval.	**pim timer join-prune** *interval*	Optional. Defaults to 60 seconds.
6. Configure the join/prune timeout time.	**pim holdtime join-prune** *interval*	Optional. Defaults to 210 seconds.
7. Configure assert timeout time.	**pim holdtime assert** *interval*	Optional. Defaults to 180 seconds.

Configuring join/prune message sizes

A larger join/prune message size results in loss of a larger amount of information if a message is lost. With a reduced join/message size, the loss of a single message has a relatively minor impact.

Controlling the maximum number of (S, G) entries in a join/prune message can reduce the number of (S, G) entries sent per unit of time.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network PIM view or VPN instance PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	—
3. Configure the maximum size of a join/prune message.	**jp-pkt-size** *packet-size*	Optional. 8,100 bytes by default.
4. Configure the maximum number of (S, G) entries in a join/prune message.	**jp-queue-size** *queue-size*	Optional. 1,020 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.

Before configuring this feature on an interface, be sure to enable PIM-DM or PIM-SM on the interface.

For more information about BFD, see *High Availability Configuration Guide*.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Enable PIM to work with BFD.	**pim bfd enable**	Required. Defaults to disabled.

Displaying and maintaining PIM

To do…	Use the 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** *vpn-instance-name*] **bsr-info** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the information of unicast routes used by PIM.	**display pim** [**all-instance** | **vpn-instance** *vpn-instance-name*] **claimed-route** [*source-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the number of PIM control messages.	**display pim** [**all-instance** | **vpn-instance** *vpn-instance-name*] **control-message counters** [**message-type** { **probe** | **register** | **register-stop** } | [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **crp** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** }] *] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the DF information of BIDIR-PIM.	**display pim** [**all-instance** | **vpn-instance** *vpn-instance-name*] **df-info** [*rp-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the information about unacknowledged graft messages.	**display** [**all-instance** | **vpn-instance** *vpn-instance-name*] **pim grafts** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the PIM information on an interface or all interfaces.	**display pim** [**all-instance** | **vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the information of join/prune messages to send.	**display pim** [**all-instance** | **vpn-instance** *vpn-instance-name*] **join-prune mode** { **sm** [**flags** *flag-value*] | **ssm** } [**interface** *interface-type interface-number* | **neighbor** *neighbor-address*] * [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display PIM neighboring information.	**display pim** [**all-instance** | **vpn-instance** *vpn-instance-name*] **neighbor** [**interface** *interface-type interface-number* | *neighbor-address* | **verbose**] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

To do...	Use the command...	Remarks
Display the content of the PIM routing table.	**display pim** [**all-instance** | **vpn-instance** *vpn-instance-name*] **routing-table** [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** [*interface-type interface-number* | **register**] | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** } | **mode** *mode-type* | **flags** *flag-value* | **fsm**] * [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the RP information.	**display pim** [**all-instance** | **vpn-instance** *vpn-instance-name*] **rp-info** [*group-address*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Reset PIM control message counters.	**reset pim** [**all-instance** | **vpn-instance** *vpn-instance-name*] **control-message counters** [**interface** *interface-type interface-number*]	Available in user view.

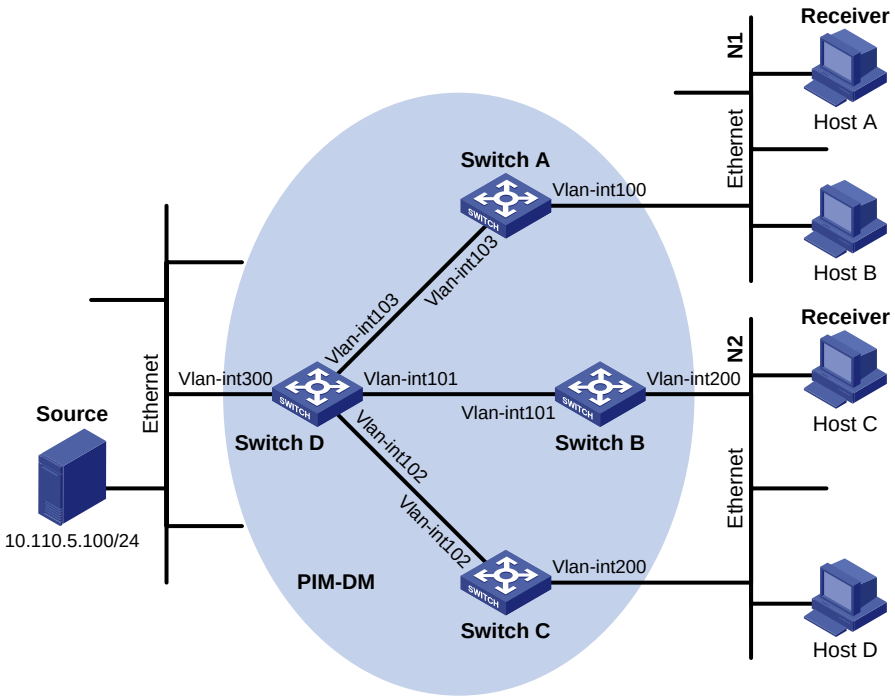
PIM configuration examples

PIM-DM configuration example

Network requirements

- As shown in Figure 50, 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 operates in the dense mode.
- Host A and Host C are multicast receivers in two stub networks.
- Switch D connects to the network that comprises the multicast source (Source) through VLAN-interface 300.
- Switch A connects to stub network N1 through VLAN-interface 100, and to Switch D through VLAN-interface 103.
- Switch B and Switch C connect to stub network N2 through their respective VLAN-interface 200, and to Switch D through VLAN-interface 101 and VLAN-interface 102 respectively.
- IGMPv2 will run between Switch A and N1, and between Switch B/Switch C and N2.

Figure 50 Network diagram for PIM-DM configuration



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			

Procedure

1. Configure the IP address and subnet mask for each interface as shown in Figure 50. Detailed configuration steps are omitted here.
2. Configure OSPF on the switches in the PIM-DM domain to ensure network-layer reachability among them. Detailed configuration steps are omitted here.
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, which connects Switch A to the stub network.

```
<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
```

The configuration on Switch B and Switch C is similar to that on Switch A.

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
```

4. Verify the configuration

Use the **display pim interface** command to view the PIM configuration and running status on each interface. For example:

View the 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)
```

Carry out the **display pim neighbor** command to view the PIM neighboring relationships among the switches. For example:

View the 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. Use the **display pim routing-table** command to view the PIM routing table information on each switch. For example:

View the 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
```

The information on Switch B and Switch C is similar to that on Switch A.

View the PIM routing table information on Switch D.

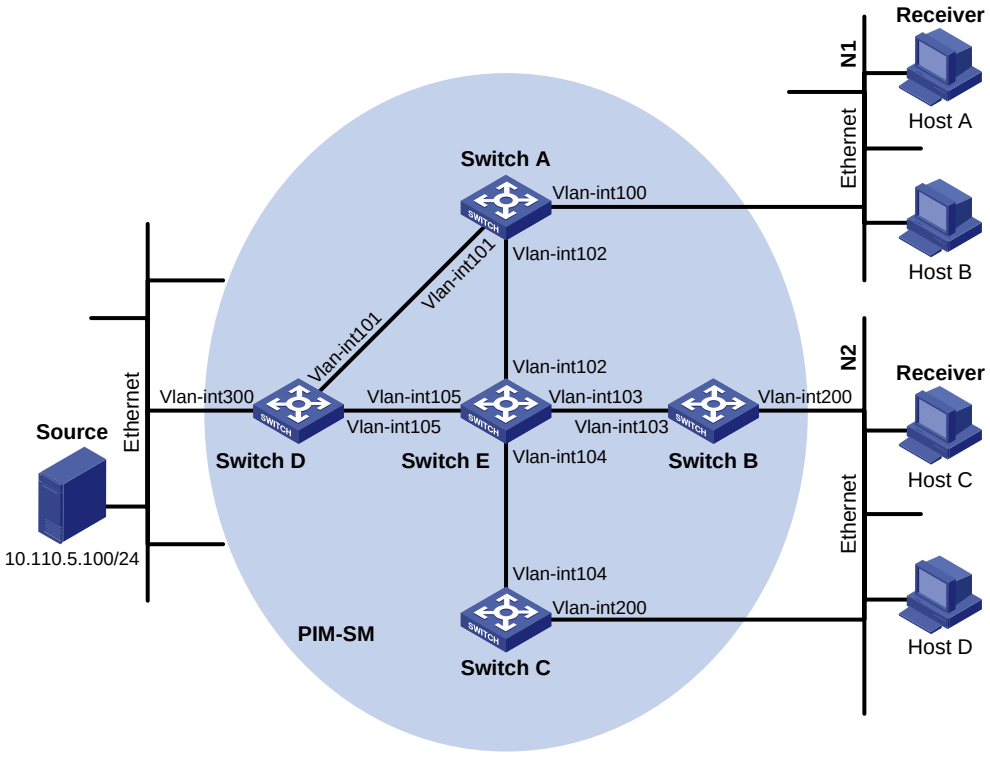
```
[SwitchD] display pim routing-table
 VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

 (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: 3
         1: Vlan-interface103
             Protocol: pim-dm, UpTime: 00:03:27, Expires: never
         2: Vlan-interface101
             Protocol: pim-dm, UpTime: 00:03:27, Expires: never
         3: Vlan-interface102
             Protocol: pim-dm, UpTime: 00:03:27, Expires: never
```

PIM-SM non-scoped zone configuration example

Network requirements

- As shown in Figure 51, 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.
- Switch D connects to the network that comprises the multicast source (Source) through VLAN-interface 300.
- Switch A connects to stub network N1 through VLAN-interface 100, and to Switch D and Switch E through VLAN-interface 101 and VLAN-interface 102 respectively.
- Switch B and Switch C connect to stub network N2 through their respective VLAN-interface 200, and to Switch E through VLAN-interface 103 and VLAN-interface 104 respectively.
- 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 served by the C-RP 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 51 Network diagram for PIM-SM non- scoped zone configuration



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

Procedure

1. Configure the IP address and subnet mask for each interface as shown in Figure 51. Detailed configuration steps are omitted here.
2. Configure OSPF on the switches in the PIM-SM domain to ensure network-layer reachability among them. Detailed configuration steps are omitted here.
3. Enable IP multicast routing, and enable PIM-SM and IGMP

Enable IP multicast routing on Switch A, enable PIM-SM on each interface, and enable IGMP on VLAN-interface 100, which connects Switch A to the stub network.

```
<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
```

The configuration on Switch B and Switch C is similar to that on Switch A. The configuration on Switch D and Switch E is also similar to that on Switch A except that it is not necessary to enable IGMP on the corresponding interfaces on these two switches.

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
```

5. Verify the configuration

Carry out the **display pim interface** command to view the PIM configuration and running status on each interface. For example:

View the 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
```

To view the BSR election information and the locally configured C-RP information in effect on a switch, use the **display pim bsr-info** command. For example:

View the 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
```

View the 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
```

View the 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
```

To view the RP information discovered on a switch, use the **display pim rp-info** command. For example:

View the 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. Upon 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, but the switches on the SPT path (Switch A and Switch D) have an (S, G) entry. Use the **display pim routing-table** command to view the PIM routing table information on the switches. For example:

View the 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.

View the 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
```

View the PIM routing table information on Switch E.

```
[SwitchE] display pim routing-table
```

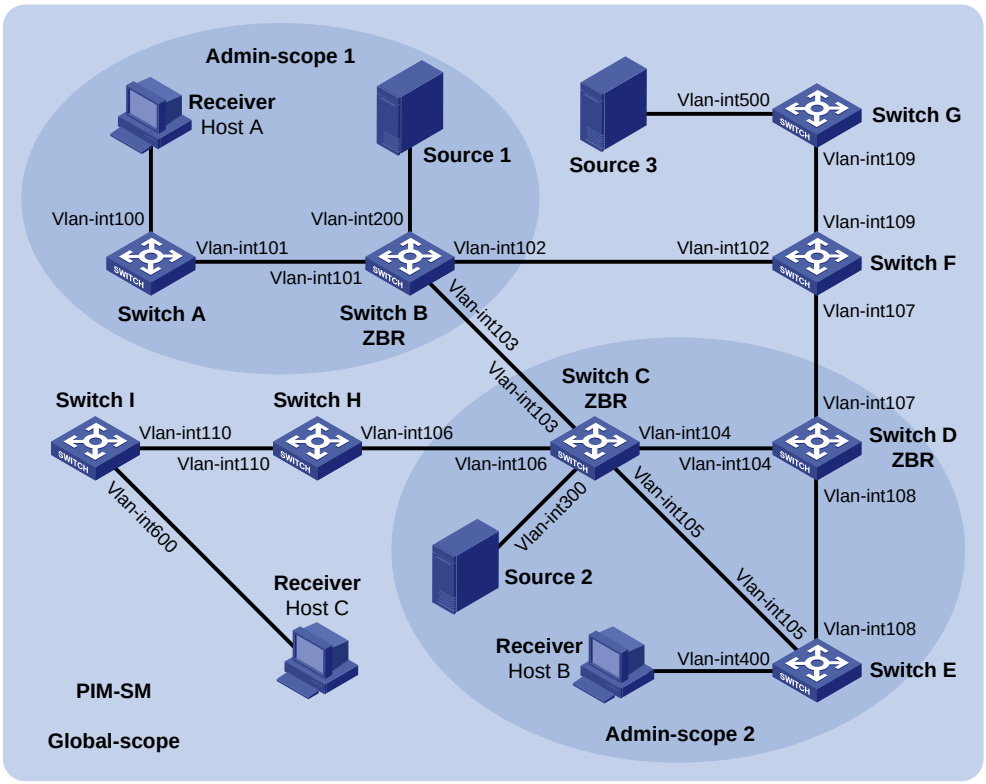
```
VPN-Instance: public net
Total 1 (*, G) entry; 0 (S, G) entry

(*, 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 52, 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 from only Source 1, and Host B receives the multicast information from only 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 serve 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 serve 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 serve all the multicast groups other than those in the 239.0.0.0/8 range.
- IGMPv2 is required between Switch A, Switch E, Switch I and their respective receivers.

Figure 52 Network diagram for PIM-SM admin-scope zone configuration



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		Vlan-int107	10.110.8.1/24
	Vlan-int101	10.110.1.2/24	Switch E	Vlan-int400	192.168.4.1/24
	Vlan-int103	10.110.2.1/24		Vlan-int105	10.110.5.2/24
	Vlan-int102	10.110.3.1/24		Vlan-int108	10.110.7.2/24
Switch C	Vlan-int300	192.168.3.1/24	Switch F	Vlan-int109	10.110.9.1/24
	Vlan-int104	10.110.4.1/24		Vlan-int107	10.110.8.2/24
	Vlan-int105	10.110.5.1/24		Vlan-int102	10.110.3.2/24
	Vlan-int103	10.110.2.2/24	Switch G	Vlan-int500	192.168.5.1/24
	Vlan-int106	10.110.6.1/24		Vlan-int109	10.110.9.2/24
Switch H	Vlan-int110	10.110.10.1/24	Source 1	—	192.168.2.10/24
	Vlan-int106	10.110.6.2/24	Source 2	—	192.168.3.10/24
Switch I	Vlan-int600	192.168.6.1/24	Source 3	—	192.168.5.10/24
	Vlan-int110	10.110.10.2/24			

Procedure

1. Configure the IP address and subnet mask for each interface as shown in Figure 52. The detailed configuration steps are omitted here.

2. Configure OSPF on the switches in the PIM-SM domain to ensure network-layer reachability among them. Detailed configuration steps are omitted here.
3. Enable IP multicast routing and administrative scoping, and enable PIM-SM and IGMP

Enable IP multicast routing and administrative scoping on Switch A, enable PIM-SM on each interface, and enable IGMP on the host-side interface VLAN-interface 100.

```
<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
```

The configuration on Switch E and Switch I is similar to the configuration on Switch A.

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
```

The configuration on Switch C, Switch D, Switch F, Switch G, and Switch H is similar to the configuration on Switch B. The specific configuration steps are omitted here.

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
```

6. Verify the configuration

To view the BSR election information and the C-RP information on a switch, use the **display pim bsr-info** command. For example:

View the 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
```

View the 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
```

View the 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
```

To view the RP information learned on a switch, use the **display pim rp-info** command. For example:

View the 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
```

View the 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
```

View the RP information on Switch F.

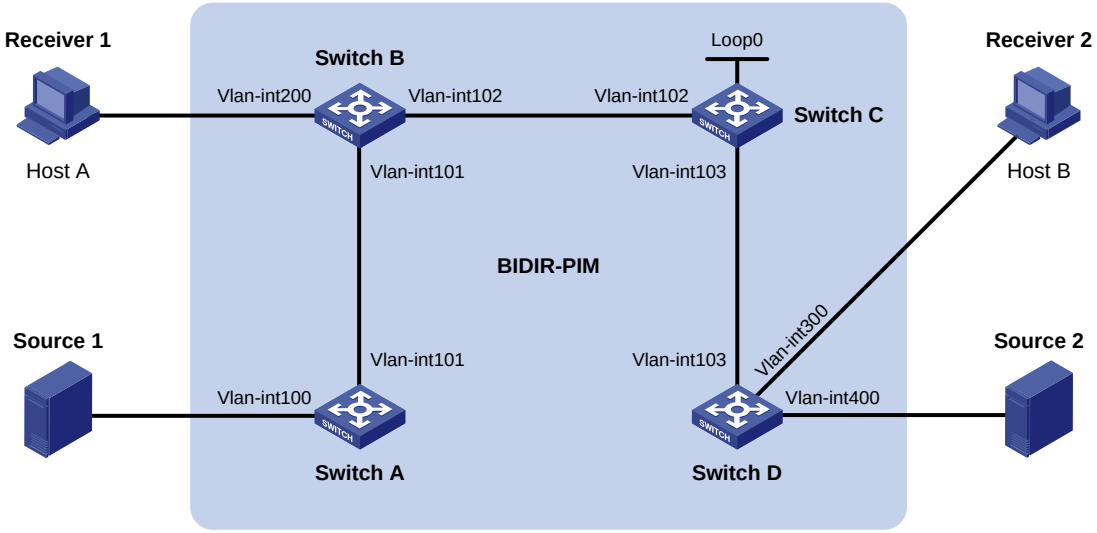
```
[SwitchF] display pim rp-info
 VPN-Instance: public net
 PIM-SM BSR RP information:
 Group/MaskLen: 224.0.0.0/4
     RP: 10.110.9.1 (local)
     Priority: 192
     HoldTime: 150
     Uptime: 00:00:32
     Expires: 00:01:58
```

BIDIR-PIM configuration example

Network requirements

- In the BIDIR-PIM domain shown in Figure 53. 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 acts as a C-RP of the BIDIR-PIM domain.
- IGMPv2 will run between Switch B and Host A, and between Switch D and Host B.

Figure 53 Network diagram for BIDIR-PIM configuration



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			

Procedure

1. Configure the IP address and subnet mask for each interface as shown in Figure 53. The configuration steps are omitted here.
2. Configure OSPF on the switches in the BIDIR-PIM domain to ensure network-layer reachability among them. The configuration steps are omitted here.
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 on 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 on 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. Configure C-BSR and C-RP

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
```

5. Verify the configuration

To view the DF information of BIDIR-PIM on a switch, use the **display pim df-info** command:

View 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
```

View 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
```

View 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)
```

View 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
```

To view the DF information of the multicast forwarding table on a switch, use the **display multicast forwarding-table df-info** command. For more information about this command, see the *IP Multicast Command Reference*.

View 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
```

View 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
```

View 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
```

View 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
```

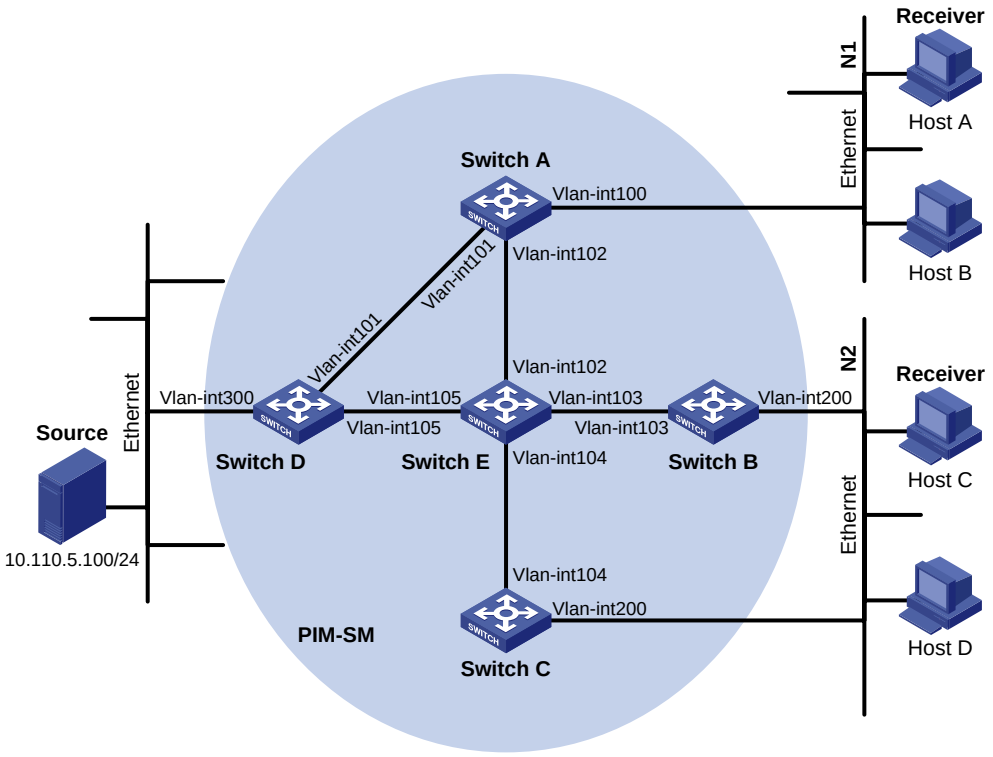
```
Total 1 RP

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 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 domain operates in the SSM mode.
- Host A and Host C are multicast receivers in two stub networks.
- Switch D connects to the network that comprises the multicast source (Source) through VLAN-interface 300.
- Switch A connects to stub network N1 through VLAN-interface 100, and to Switch D and Switch E through VLAN-interface 101 and VLAN-interface 102 respectively.
- Switch B and Switch C connect to stub network N2 through their respective VLAN-interface 200, and to Switch E through VLAN-interface 103 and VLAN-interface 104 respectively.
- Switch E connects to Switch A, Switch B, Switch C and Switch D.
- 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 54 Network diagram for PIM-SSM configuration



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

Procedure

1. Configure the IP address and subnet mask for each interface as shown in Figure 54. Detailed configuration steps are omitted here.
2. Configure OSPF on the switches in the PIM-SM domain to ensure network-layer reachability among them. Detailed configuration steps are omitted here.
3. Enable IP multicast routing, and enable PIM-SM and IGMP

Enable IP multicast routing on Switch A, enable PIM-SM on each interface, and run IGMPv3 on VLAN-interface 100, which connects Switch A to the stub network.

```
<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
```

The configuration on Switch B and Switch C is similar to that on Switch A. The configuration on Switch D and Switch E is also similar to that on Switch A except that it is not necessary to enable IGMP on the corresponding interfaces on these two switches.

4. Configure the SSM group range

Configure the SSM group range to be 232.1.1.0/24 one 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
```

The configuration on Switch B, Switch C, Switch D and Switch E is similar to that on Switch A.

5. Verify the configuration

Carry out the **display pim interface** command to view the PIM configuration and running status on each interface. For example:

View the 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. The 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. Use the **display pim routing-table** command to view the PIM routing table information on each switch. For example:

View the 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
```

The information on Switch B and Switch C is similar to that on Switch A.

View the 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 configuration

Failure of building a multicast distribution tree correctly

Symptom

None of the routers in the network (including routers directly connected with multicast sources and receivers) has multicast forwarding entries. 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, no matter which router is, it 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 joins 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 router 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 running PIM is unable to know 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 surely fail, causing abnormal multicast forwarding.
- The same PIM mode must run on the entire network. Otherwise, the establishment of a multicast distribution tree will surely fail, causing abnormal multicast forwarding.

Solution

1. Verify unicast routes. Use the **display ip routing-table** command to determine whether a unicast route exists from the receiver host to the multicast source.
2. Verify that PIM is enabled on the interfaces, especially on the RPF interface. Use the **display pim interface** command to determine the PIM information on each 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. Verify that the RPF neighbor is a PIM neighbor. Use the **display pim neighbor** command to view the PIM neighbor information.
4. Verify that PIM and IGMP are enabled on the interfaces that are directly connected to the multicast source and to the receivers.
5. Verify that the same PIM mode is enabled on related interfaces. Use the **display pim interface verbose** command to determine whether 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 (PIM-SM or PIM-DM) is enabled on all the routers in the entire network. Make sure that the same PIM mode is enabled on all the routers. In the case of PIM-SM, also verify 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 using the **multicast boundary** command, any multicast packet is 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 defined in this command, PIM cannot create the route entry, either.

Solution

1. Verify the multicast forwarding boundary configuration. Use the **display current-configuration** command to determine the multicast forwarding boundary settings. Use the **multicast boundary** command to change the multicast forwarding boundary settings.
2. Verify the multicast filter configuration. Use the **display current-configuration** command to determine the multicast filter configuration. Change the ACL defined in the **source-policy** command so that the source/group address of the multicast data can pass ACL filtering.

RPs unable to 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 serve specific multicast groups. Multiple RPs can coexist in a network. Make sure that the RP information on all routers is exactly the same, and 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. Verify that a route is available to the RP. Use the **display ip routing-table** command to determine whether a route is available on each router to the RP.
2. Verify the dynamic RP information. Use the **display pim rp-info** command to determine whether the RP information is consistent on all routers.
3. Verify the configuration of static RPs. Use the **display pim rp-info** command to determine whether 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 register 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 information about that C-RP.
- If the BSR does not have a unicast router to a C-RP, it will discard the C-RP-Adv messages from that C-RP. Therefore the bootstrap messages of the BSR will not contain information about 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. Verify that the routes to C-RPs and the BSR are available. Use the **display ip routing-table** command to determine whether the 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. Verify the RP and BSR information. PIM-SM needs the support of the RP and BSR. Use the **display pim bsr-info** command to determine whether the BSR information is available on each router, and then use the **display pim rp-info** command to determine whether the RP information is correct.

3. Verify the PIM neighboring relationships. Use the **display pim neighbor** command to determine whether the normal PIM neighboring relationships have been established among the routers.

Configuring MSDP

For more information about the concepts of DR, BSR, C-BSR, RP, C-RP, SPT, and RPT, see *IP Multicast Configuration Guide*.

MSDP is an inter-domain multicast solution that addresses the interconnection of PIM-SM domains. You can use it to discover multicast source information in other PIM-SM domains.

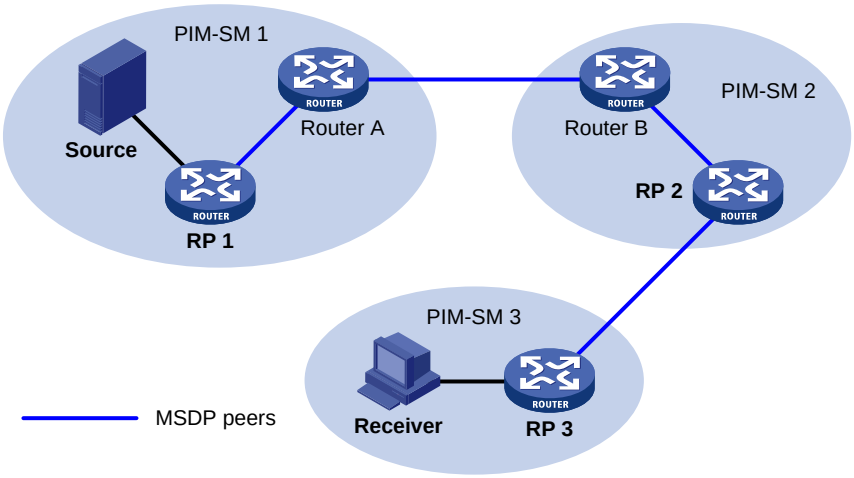
In the basic PIM-SM mode, a multicast source registers only with the RP in the local PIM-SM domain, and the multicast source information about a domain is isolated from that of another domain. As a result, the RP detects the source information only within the local domain and a multicast distribution tree is built only within the local domain to deliver multicast data from a local multicast source to local receivers. If a mechanism allows RPs of different PIM-SM domains to share their multicast source information, the local RP will be able to join multicast sources in other domains and multicast data can be transmitted among different domains.

MSDP achieves this goal. Establishing MSDP peer relationships between appropriate routers in the network interconnects the RPs of different PIM-SM domains. These MSDP peers exchange SA messages, so the multicast source information is shared among these different domains.

MSDP is applicable only if the intra-domain multicast protocol is PIM-SM. MSDP is meaningful only for the any-source multicast (ASM) model.

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 sent by an RP and relayed by these MSDP peers can be delivered to all other RPs.

Figure 55 Where MSDP peers are in the network



As shown in Figure 55, an MSDP peer can be created on any PIM-SM router. MSDP peers created on PIM-SM routers that assume different roles function differently.

MSDP peers on RPs include the following:

- 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 is unable 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. Upon 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.

MSDP peers can also be created on common PIM-SM routers (other than RPs).

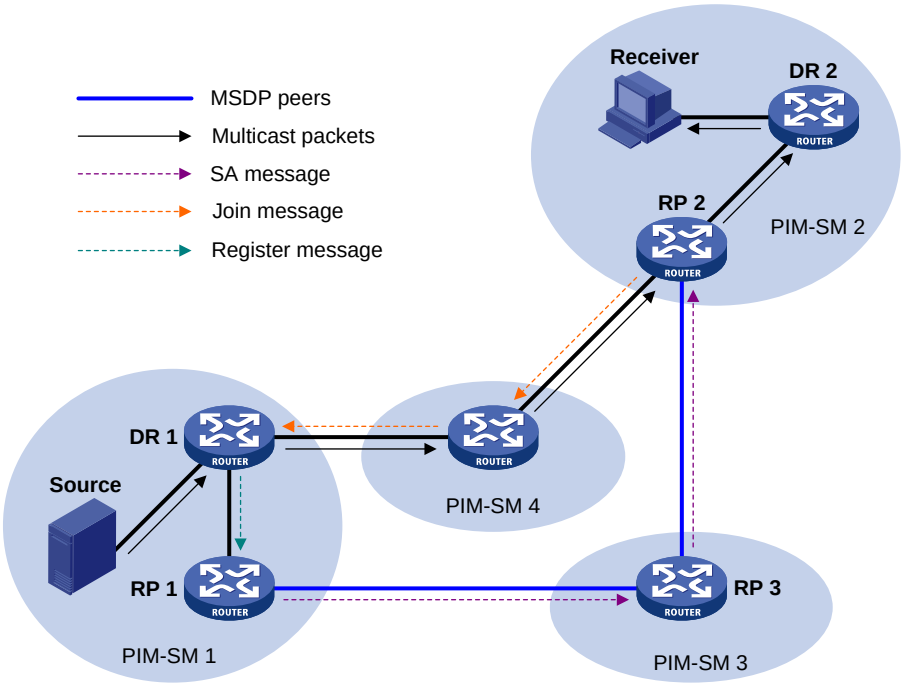
Router A and Router B are MSDP peers on common multicast routers. Such MSDP peers just forward received SA messages.

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 relationships should be built among all C-RPs so that the winner C-RP is always on the "MSDP interconnection map", while loser C-RPs will assume the role of common PIM-SM routers on the "MSDP interconnection map".

Implementing inter-domain multicast delivery

As shown in Figure 56, an active source (Source) exists in the domain PIM-SM 1, and RP 1 has identified 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 originated from it, HP recommends establishing MSDP peer relationships between RP 1 and RP 3 and between RP 3 and RP 2 respectively.

Figure 56 MSDP peering relationships



The process of implementing 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 (RP 1).
3. On MSDP peers, each SA message undergoes an RPF verification 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, configure MSDP peers into an MSDP mesh group to avoid flooding of SA messages between MSDP peers.
4. SA messages are forwarded from one MSDP peer to another, and finally information about the multicast source traverses all PIM-SM domains with MSDP peers (PIM-SM 2 and PIM-SM 3 in this example).
5. Upon 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 so, 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 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.

An MSDP mesh group refers to a group of MSDP peers that have MSDP peering relationships among one another and share the same group name.

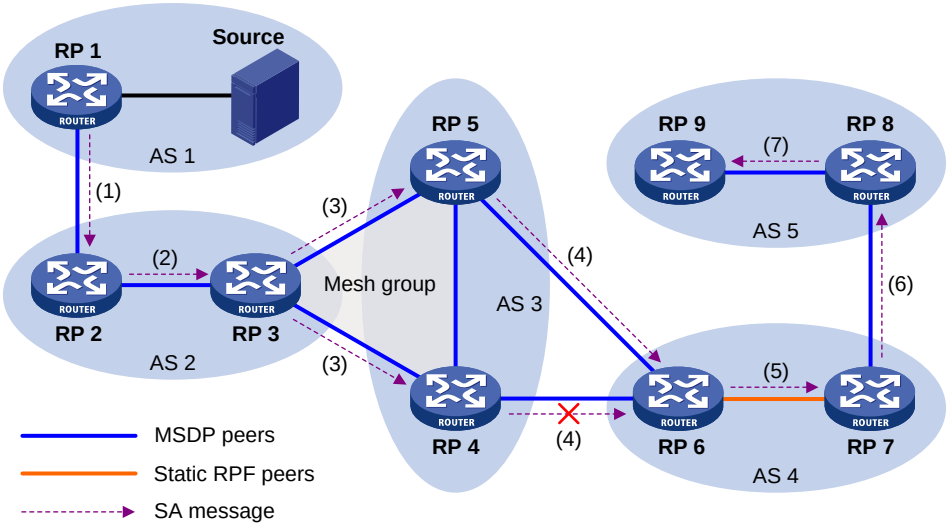
When using MSDP for inter-domain multicasting, once an RP receives information form a multicast source, it no longer relies on RPs in other PIM-SM domains. The receivers can override the RPs in other domains and directly join the multicast source-based SPT.

Checking for SA messages, RPF check rules

As shown in Figure 57, autonomous systems AS 1 through AS 5 enable IGP on routers within each AS and enable 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 ore more RPs. MSDP peer relationships have 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.

If only one MSDP peer exists in a PIM-SM domain, this PIM-SM domain is also called a stub domain. For example, AS 4 in is a stub domain. The MSDP peer in a stub domain can have multiple remote MSDP peers at the same time. You can configure one or more remote MSDP peers as static RPF peers. 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 57 Figure Diagram for RPF check for SA messages



As illustrated in Figure 57, these MSDP peers dispose of SA messages according to the following RPF verification rules:

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).

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).

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.

When RP 6 receives the SA messages from RP 4 and RP 5 (suppose 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.

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).

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).

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 other paths are not accepted or forwarded by MSDP peers.

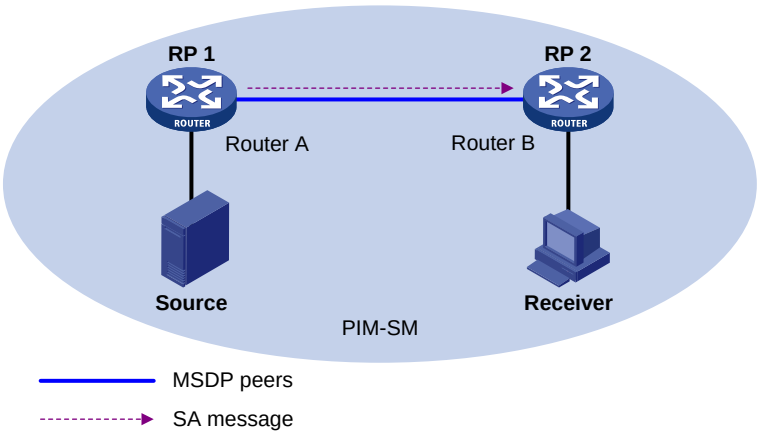
Implementing intra-domain Anycast RP by leveraging MSDP peers

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 peer relationships between, these RPs.

As shown in Figure 58, 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 peer relationship between Router A and Router B.

Usually an Anycast RP address is configured on a logic interface, like a loopback interface.

Figure 58 Figure Typical network diagram of Anycast RP



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 needs to maintain just part of the source/group information within the PIM-SM domain and forward part of the multicast data, thus 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, register with or join another nearest RP, achieving redundancy backup between RPs.

Be sure to configure a 32-bit subnet mask (255.255.255.255) for the Anycast RP address (configure the Anycast RP address into a host address).

An MSDP peer address must be different from the Anycast RP address.

Multi-instance MSDP

You can build an MSDP peer relationship between multicast-enabled interfaces that belong to the same instance. Through exchanges of SA messages between MSDP peers, the MSDP mechanism enables VPN multicast transmission between different PIM-SM domains.

A multicast router that runs multiple MSDP instances maintains an independent set of MSDP mechanisms for each instance that it supports, including SA cache, peer connection, timers, sending cache, and cache for exchanging information with PIM. However, these instances are isolated from one another. Interoperability between MSDP and PIM-SM is available only within the same instance.

Protocols and standards

MSDP is documented in the following specifications:

- 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)*

Configuring basic functions of MSDP

All the configuration tasks should be carried out on RPs in PIM-SM domains, and each of these RPs acts as an MSDP peer.

Prerequisites

Before configuring the basic functions of MSDP, 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

Enabling MSDP globally for the public network

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enable IP multicast routing.	**multicast routing-enable**	Required. Defaults to disabled.

To do...	Use the command...	Remarks
3. Enable MSDP and enter public network MSDP view.	**msdp**	Required. Defaults to disabled.

Enabling MSDP in a VPN instance

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Create a VPN instance and enter VPN instance view.	**ip vpn-instance** *vpn-instance-name*	—
3. Configure a route-distinguisher (RD) for the VPN instance.	**route-distinguisher** *route-distinguisher*	Required. No RD is configured by default.
4. Enable IP multicast routing.	**multicast routing-enable**	Required. Defaults to disabled.
5. Return to system view.	**quit**	—
6. Enable MSDP and enter VPN instance MSDP view.	**msdp vpn-instance** *vpn-instance-name*	Required. Defaults to disabled.

For more information about **ip vpn-instance** and **route-distinguisher**, see *MPLS Command Reference*.

For more information about **multicast routing-enable**, see *IP Multicast Command Reference*.

Creating an MSDP peer connection

An MSDP peering relationship is identified by an address pair (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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network MSDP view or VPN instance MSDP view.	**msdp** [**vpn-instance** *vpn-instance-name*]	—
3. Create an MSDP peer connection.	**peer** *peer-address* **connect-interface** *interface-type interface-number*	Required. No MSDP peer connection created by default.

If an interface of the router is shared by an MSDP peer and a BGP/MBGP peer at the same time, we recommend that you use the IP address of the BGP/MBGP peer as the IP address of the for the MSDP peer.

Configuring a static RPF peer

Configuring static RPF peers avoids RPF check of SA messages.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—

To do...	Use the command...	Remarks
2. Enter public network MSDP view or VPN instance MSDP view.	**msdp** [**vpn-instance** *vpn-instance-name*]	—
3. Configure a static RPF peer.	**static-rpf-peer** *peer-address* [**rp-policy** *ip-prefix-name*]	Required. No static RPF peer configured by default.

If only one MSDP peer is configured on a router, this MSDP is registered as a static RPF peer.

Configuring an MSDP peer connection

Prerequisites

Before configuring 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.
- Configuring basic functions of MSDP
- Determine the description information of MSDP peers
- Determine the name of an MSDP mesh group
- Determine the MSDP peer connection retry interval

Configuring MSDP peer description

With the MSDP peer description information, the administrator can easily distinguish different MSDP peers and thus better manage MSDP peers.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network MSDP view or VPN instance MSDP view.	**msdp** [**vpn-instance** *vpn-instance-name*]	—
3. Configure description for an MSDP peer.	**peer** *peer-address* **description** *text*	Required. No description for MSDP peers 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 from outside the mesh group (that have passed the RPF verification) to the other members in the mesh group. A mesh group member accepts SA messages from inside the group without performing an RPF verification, and does not forward the message within the mesh group. This mechanism avoids SA flooding and simplifies the RPF verification mechanism, because there is no 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.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network MSDP view or VPN instance MSDP view.	**msdp** [**vpn-instance** *vpn-instance-name*]	—
3. Create an MSDP mesh group and assign an MSDP peer to that mesh group.	**peer** *peer-address* **mesh-group** *name*	Required. An MSDP peer does not belong to any mesh group by default.

Before grouping multiple routers into an MSDP mesh group, make sure that these routers are interconnected with one another.

If you configure more than one mesh group name on an MSDP peer, only the last configuration is effective.

Configuring MSDP peer connection control

MSDP peers are interconnected over TCP with port number 639. You can control the sessions between MSDP peers by deactivating and reactivating the MSDP peer 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 remains unchanged.

When you create a new MSDP peer, or when you reactivate a previously deactivated MSDP peer connection, or when a previously failed MSDP peer attempts to resume operation, a TCP connection is required. You can adjust the interval between MSDP peer connection retries.

Follow these steps to configure MSDP peer connection control:

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network MSDP view or VPN instance MSDP view.	**msdp** [**vpn-instance** *vpn-instance-name*]	—
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. Defaults to 30 seconds.

Configuring SA messages related parameters

Prerequisites

Before configuring 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

- Configuring basic functions of MSDP
- 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. 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.

If the source-side RP is enabled to encapsulate register messages in SA messages, when there is a multicast packet to deliver, the source-side RP encapsulates a register message that contains the multicast packet in an SA message and sends it. After receiving the SA message, the remote RP decapsulates the SA message and delivers the multicast data contained in the register message to the receivers along the RPT.

The MSDP peers deliver SA messages to one another. Upon receiving an SA message, a switch performs RPF verification on the message. If the switch 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 devices in the same PIM-SM domain, and configure these devices as MSDP peers to one another. Therefore, a logic RP address (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 verification.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network MSDP view or VPN instance MSDP view.	**msdp** [**vpn-instance** *vpn-instance-name*]	—
3. Enable encapsulation of a register message.	**encap-data-enable**	Optional. Defaults to disabled.
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 switch does not send an SA request message to any MSDP peer. Instead, it waits for the next SA message from its MSDP peer. This causes the receiver to delay obtaining multicast source information. To enable a new receiver to get the currently active multicast source information as early as possible, configure devices to send SA request messages to the designated MSDP peers upon receiving a join message of a new receiver.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network MSDP view or VPN instance MSDP view.	**msdp** [**vpn-instance** *vpn-instance-name*]	—
3. Enable the device to send SA request messages.	**peer** *peer-address* **request-sa-enable**	Optional. Defaults to disabled.
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.

Before you can enable the device to send SA requests, be sure to disable the SA message cache mechanism.

Configuring SA message filtering rules

By configuring an SA message creation rule, you can enable the switch 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 switch 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 switch identifies the TTL value of the multicast data packet. If the TTL value is less than the threshold, the switch does not create an SA message. If the TTL value is greater than or equal to the threshold, the switch encapsulates the multicast data in an SA message and sends the SA message.
- Upon receiving an SA message with an encapsulated multicast data packet, the switch decrements the TTL value of the multicast packet by 1, and then identifies the TTL value. If the TTL value is less than the threshold, the switch does not forward the SA message to the designated MSDP peer. If the TTL value is greater than or equal to the threshold, the switch re-encapsulates the multicast data in an SA message and sends the SA message.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network MSDP view or VPN instance MSDP view.	**msdp** [**vpn-instance** *vpn-instance-name*]	—
3. Configure an SA message creation rule.	**import-source** [**acl** *acl-number*]	Required. 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*]	Required. No filtering rule by default.

To do...	Use the command...	Remarks
5. Configure the TTL threshold for multicast data packet encapsulation in SA messages.	**peer** *peer-address* **minimum-ttl** *ttl-value*	Optional. Defaults to 0.

Configuring the SA cache mechanism

To reduce the time spent in obtaining the multicast information, enable the SA cache mechanism to cache (S, G) entries contained in SA messages locally on the switch. However, caching (S, G) entries uses memory space on the switch.

When the SA cache mechanism is enabled and the switch receives a new (*, G) join message, the switch searches its SA cache first.

- If the corresponding (S, G) entry does not exist in the cache, the switch 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 switch joins the corresponding SPT rooted at S.

To protect the switch effectively against DoS attacks, set a limit on the number of (S, G) entries the switch can cache.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter public network MSDP view or VPN instance MSDP view.	**msdp** [**vpn-instance** *vpn-instance-name*]	—
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 switch can cache.	**peer** *peer-address* **sa-cache-maximum** *sa-limit*	Optional. Defaults to 8192.

Displaying and maintaining MSDP

To do...	Use the command...	Remarks
View the brief information of 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.
View the 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.
View 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.

To do...	Use the command...	Remarks
View 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.
Reset the TCP connection with an MSDP peer.	**reset msdp** [**all-instance** | **vpn-instance** *vpn-instance-name*] **peer** [*peer-address*]	Available in user view.
Clear (S, G) entries in the SA cache.	**reset msdp** [**all-instance** | **vpn-instance** *vpn-instance-name*] **sa-cache** [*group-address*]	Available in user view.
Clear all statistics information of an MSDP peer.	**reset msdp** [**all-instance** | **vpn-instance** *vpn-instance-name*] **statistics** [*peer-address*]	Available in user view.

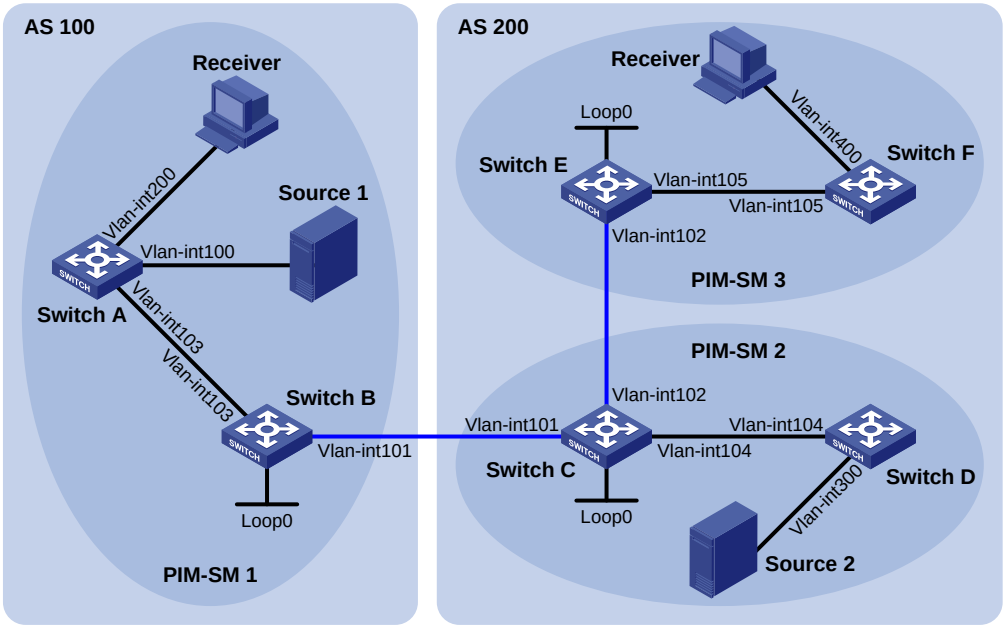
MSDP configuration examples

Inter-AS multicast configuration leveraging BGP routes

Network requirements

- As shown in Figure 59, 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 zero or one multicast source and receiver. OSPF runs within each domain to provide unicast routes.
- Configure the respective Loopback 0 of Switch B, Switch C, and Switch E as the C-BSR and C-RP of the respective PIM-SM domains.
- Set up an MSDP peer relationship between Switch B and Switch C through EBGP, and between Switch C and Switch E through IBGP.

Figure 59 Network diagram for inter-AS multicast configuration leveraging BGP routes



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			

Procedure

1. Configure the IP address and subnet mask for each interface as shown in Figure 59. Detailed configuration steps are omitted here.
2. Configure OSPF for interconnection between switches in each AS. Ensure the network-layer interoperation among each AS, and ensure the dynamic update of routing information between the switches through a unicast routing protocol. Detailed configuration steps are omitted here.
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
```

The configuration on Switch B, Switch C, Switch D, Switch E, and Switch F is similar to the configuration on Switch A.

Configure a PIM domain border on Switch B.

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim bsr-boundary
[SwitchB-Vlan-interface101] quit
```

The configuration on Switch C and Switch E is similar to the configuration on Switch B.

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
```

The configuration on Switch C and Switch E is similar to the configuration on Switch B.

5. Configure BGP for mutual route redistribution between BGP and OSPF

Configure EBGP on Switch B, and redistribute OSPF routes.

```
[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 IBGP and EBGP on Switch C, and redistribute OSPF routes.

```
[SwitchC] bgp 200
[SwitchC-bgp] router-id 2.2.2.2
[SwitchC-bgp] peer 192.168.1.1 as-number 100
[SwitchC-bgp] peer 192.168.3.2 as-number 200
[SwitchC-bgp] import-route ospf 1
[SwitchC-bgp] quit
```

Configure IBGP on Switch E, and redistribute OSPF routes.

```
[SwitchE] bgp 200
[SwitchE-bgp] router-id 3.3.3.3
[SwitchE-bgp] peer 192.168.3.1 as-number 200
[SwitchE-bgp] import-route ospf 1
[SwitchE-bgp] quit
```

Redistribute BGP routes into OSPF on Switch B.

```
[SwitchB] ospf 1
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] quit
```

The configuration on Switch C and Switch E is similar to the configuration on Switch B.

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
```

7. Verify the configuration

Use the **display bgp peer** command to view the BGP peering relationships between the switches. For example:

View the information about BGP peering relationships 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         V            AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State

  192.168.1.2  4           200       24       21     0       6 00:13:09 Established
```

View the information about BGP peering relationships on Switch C.

```
[SwitchC] display bgp peer

 BGP local router ID : 2.2.2.2
 Local AS number : 200
 Total number of peers : 2                 Peers in established state : 2

  Peer         V            AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State

  192.168.1.1  4           100       18       16     0       1 00:12:04 Established
  192.168.3.2  4           200       21       20     0       6 00:12:05 Established
```

View the information about BGP peering relationships on Switch E.

```
[SwitchE] display bgp peer
```

```
BGP local router ID : 3.3.3.3
 Local AS number : 200
 Total number of peers : 1                 Peers in established state : 1

  Peer         V            AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State

  192.168.3.1  4           200       16       14     0       1 00:10:58 Established
```

To view the BGP routing table information on the switches, use the **display bgp routing-table** command. For example:

View the BGP routing table information on Switch C.

```
[SwitchC] display bgp routing-table

 Total Number of Routes: 13

 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         192.168.3.2     0          100        0       ?
 * >   3.3.3.3/32         0.0.0.0         0                     0       ?
 * >   192.168.1.0        0.0.0.0         0                     0       ?
 *                       192.168.1.1     0                     0       100?
 * >   192.168.1.1/32     0.0.0.0         0                     0       ?
 * >   192.168.1.2/32     0.0.0.0         0                     0       ?
 *                       192.168.1.1     0                     0       100?
 * >   192.168.3.0        0.0.0.0         0                     0       ?
 * i                     192.168.3.2     0          100        0       ?
 * >   192.168.3.1/32     0.0.0.0         0                     0       ?
 * >   192.168.3.2/32     0.0.0.0         0                     0       ?
 * i                     192.168.3.2     0          100        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. Use **display msdp brief** to view the brief information of MSDP peering relationships between the switches. For example:

View the brief information about MSDP peering relationships 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
```

View the brief information about MSDP peering relationships 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
```

View the brief information about MSDP peering relationships 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
```

View the detailed MSDP peer information on Switch B.

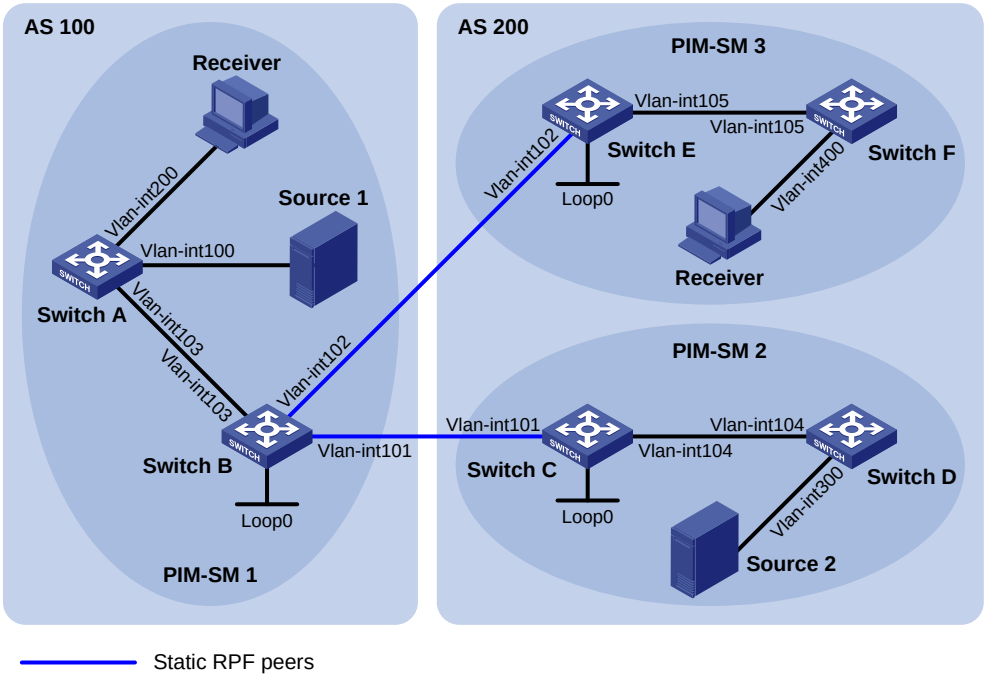
```
[SwitchB] display msdp peer-status
MSDP Peer Information of VPN-Instance: public net
  MSDP Peer 192.168.1.2, AS 200
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:15:47
    Resets: 0
    Connection interface: Vlan-interface101 (192.168.1.1)
    Number of 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 leveraging static RPF peers

Network requirements

- As shown in Figure 60, 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 zero or one multicast source and receiver. OSPF runs within each domain to provide unicast routes.
- PIM-SM 2 and PIM-SM 3 are both stub domains, and BGP or MBGP is not required between these two domains and PIM-SM 1. Instead, static RPF peers are configured to avoid RPF check on SA messages.
- You must configure the respective loopback 0 of Switch B, Switch C and Switch E as the C-BSR and C-RP of the respective PIM-SM domains.
- Configure Switch C and Switch E as static RPF peers of Switch B, and Switch B as the only static RPF peer of Switch C and Switch E, so that any switch can receive SA messages only from its static RPF peers and permitted by the corresponding filtering policy.

Figure 60 Network diagram for inter-AS multicast configuration leveraging static RPF peers



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
	Vlan-int102	192.168.3.1/24	Switch F	Vlan-int105	10.110.6.2/24
	Loop0	1.1.1.1/32		Vlan-int400	10.110.7.1/24

Switch C	Vlan-int101	192.168.1.2/24	Source 1	—	10.110.2.100/24
	Vlan-int104	10.110.4.1/24	Source 2	—	10.110.5.100/24
	Loop0	2.2.2.2/32			

Procedure

1. Configure the IP address and subnet mask for each interface as shown in Figure 60. Detailed configuration steps are omitted here.
2. Configure OSPF for interconnection between the switches. Ensure the network-layer interoperation in each AS, and ensure the dynamic update of routing information among the switches through a unicast routing protocol. Detailed configuration steps are omitted here.
3. Enable IP multicast routing, enable PIM-SM and IGMP, 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
```

The configuration on Switch B, Switch C, Switch D, Switch E, and Switch F is similar to the configuration on Switch A.

Configure PIM domain borders on Switch B.

```
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim bsr-boundary
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim bsr-boundary
[SwitchB-Vlan-interface101] quit
```

The configuration on Switch C and Switch E is similar to the configuration on Switch B.

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
```

The configuration on Switch C and Switch E is similar to the configuration on Switch B.

5. Configure a static RPF peer

Configure Switch C and Switch E as a static RPF peers of Switch B.

```
[SwitchB] ip ip-prefix list-df permit 192.168.0.0 16 greater-equal 16 less-equal 32
[SwitchB] msdp
[SwitchB-msdp] peer 192.168.3.2 connect-interface vlan-interface 102
[SwitchB-msdp] peer 192.168.1.2 connect-interface vlan-interface 101
[SwitchB-msdp] static-rpf-peer 192.168.3.2 rp-policy list-df
[SwitchB-msdp] static-rpf-peer 192.168.1.2 rp-policy list-df
[SwitchB-msdp] quit
```

Configure Switch B as a static RPF peer of Switch C.

```
[SwitchC] ip ip-prefix list-c permit 192.168.0.0 16 greater-equal 16 less-equal 32
[SwitchC] msdp
[SwitchC-msdp] peer 192.168.1.1 connect-interface vlan-interface 101
[SwitchC-msdp] static-rpf-peer 192.168.1.1 rp-policy list-c
[SwitchC-msdp] quit
```

Configure Switch B as a static RPF peer of Switch E.

```
[SwitchE] ip ip-prefix list-c permit 192.168.0.0 16 greater-equal 16 less-equal 32
[SwitchE] msdp
[SwitchE-msdp] peer 192.168.3.1 connect-interface vlan-interface 102
[SwitchE-msdp] static-rpf-peer 192.168.3.1 rp-policy list-c
[SwitchE-msdp] quit
```

6. Verify the configuration

Use **display bgp peer** to view the BGP peering relationships between the switches. If the command gives no output information, a BGP peering relationship has not been established between the switches.

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. Use **display msdp brief** to view the brief information of MSDP peering relationships between the switches. For example:

View the 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
  2            2            0            0            0            0

  Peer's Address    State    Up/Down time    AS     SA Count   Reset Count
  192.168.3.2       Up       01:07:08        ?      8          0
  192.168.1.2       Up       00:16:39        ?      13         0
```

View the brief MSDP peer information on Switch C.

```
[SwitchC] 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       01:07:09        ?      8          0
```

View the brief MSDP peer information on Switch E.

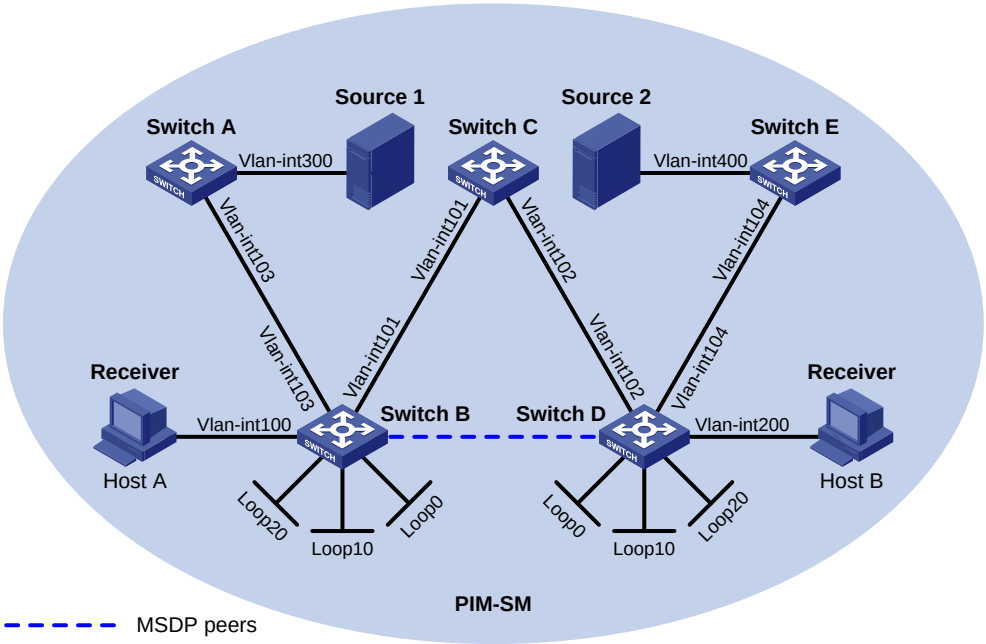
```
[SwitchE] display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
  Configured    Up            Listen        Connect       Shutdown      Down
  1             1             0             0             0             0

  Peer's Address     State     Up/Down time     AS      SA Count    Reset Count
  192.168.3.1        Up        00:16:40         ?       13          0
```

Anycast RP configuration

Network requirements

- As shown in Figure 61, 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 61 Network diagram for Anycast RP configuration



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

Procedure

1. Configure IP addresses and unicast routing

   Configure the IP address and subnet mask for each interface as shown in Figure 61. Detailed configuration steps are omitted here.

   Configure OSPF for interconnection between the switches. Ensure the network-layer interoperation among the switches, and ensure the dynamic update of routing information between the switches through a unicast routing protocol. Detailed configuration steps are omitted here.

2. Enable IP multicast routing, and enable PIM-SM and IGMP

Enable IP multicast routing on Switch B, enable PIM-SM on each interface, and enable IGMP on the host-side interface VLAN-interface 100.

```
<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
```

The configuration on Switch A, Switch C, Switch D, and Switch E is similar to the configuration on Switch B.

3. 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
```

The configuration on Switch D is similar to the configuration on Switch B.

4. 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
```

5. Verify the configuration

Use **display msdp brief** to view the brief information of MSDP peering relationships between the switches.

View the 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
```

View the 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 view the PIM routing information on the switches, use **display pim routing-table**. 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.

View the 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:  -
```

View the 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.

View the PIM routing information on Switch B.

```
[SwitchB] display pim routing-table
```

No information is output on Switch B.

View the 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)
```

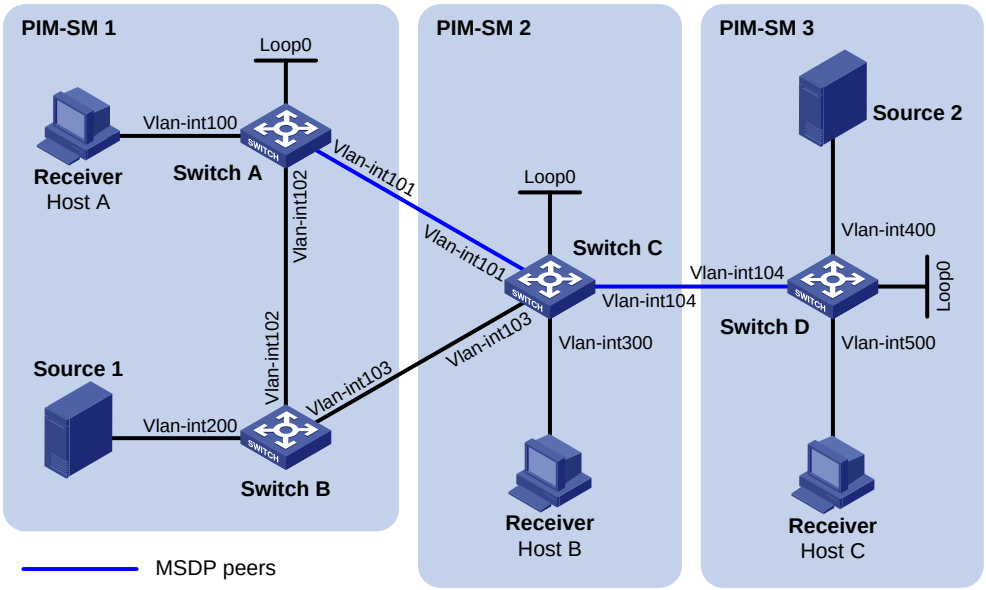
```
Protocol: pim-sm, Flag: SPT 2MSDP ACT
UpTime: 00:40:22
Upstream interface: Vlan-interface104
    Upstream neighbor: 10.110.4.2
    RPF prime neighbor: 10.110.4.2
Downstream interface(s) information:
Total number of downstreams: 1
    1: Vlan-interface200
        Protocol: pim-sm, UpTime:  - , Expires:  -
```

SA message filtering configuration

Network requirements

- As shown in Figure 62, the network has three PIM-SM domains, and OSPF runs within and among the domains to provide unicast routing.
- Configure Loopback 0 of Switch A, Switch C and Switch D as a C-BSR and C-RP in the respective PIM-SM domain.
- Set up an MSDP peering relationship 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 62 Network diagram for SA message filtering configuration



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		Vlan-int104	10.110.5.1/24
Switch A	Vlan-int100	10.110.1.1/24		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		Vlan-int500	10.110.7.1/24
	Vlan-int102	10.110.2.2/24		Vlan-int104	10.110.5.2/24
	Vlan-int103	192.168.2.1/24		Loop0	3.3.3.3/32

Configuration Procedure

1. Configure the IP address and subnet mask for each interface as shown in Figure 62. The detailed configuration steps are omitted here.
2. Configure OSPF for interoperation among the switches. Ensure the network-layer interoperation within and between the PIM-SM domains and ensure dynamic update of routing information among the switches by leveraging unicast routing. The detailed configuration steps are omitted here.
3. Enable IP multicast routing, PIM-SM and IGMP, and configure a PIM domain border

On Switch A, enable IP multicast routing, enable PIM-SM on each interface, and enable IGMP on the host-side interface, VLAN-interface 100.

```
<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
```

The configuration on Switch B, Switch C and Switch D is similar to the configuration on Switch A. The specific configuration steps are omitted here.

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
```

The configuration on Switch A, Switch B and Switch D is similar to the configuration on Switch C. The specific configuration steps are omitted here.

4. Configure C-BSRs and C-RPs

Configure Loopback 0 on Switch A as a C-BSR and a C-RP.

```
[SwitchA] pim
[SwitchA-pim] c-bsr loopback 0
[SwitchA-pim] c-rp loopback 0
[SwitchA-pim] quit
```

The configuration on Switch C and Switch D is similar to the configuration on Switch A. The specific configuration steps are omitted here.

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 entry (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
```

7. Verify the configuration

Use the **display msdp sa-cache** command to view the (S, G) entries cached in the SA cache on the switches. For example:

View 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
```

View 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 there is a consistency between the local interface address and the MSDP peer address configured on the switch.
- If no route is available between the MSDP peers, the TCP connection setup will also fail.

Solution

1. Verify that a route is available between the devices. Use the **display ip routing-table** command to determine whether the unicast route between the devices is correct.
2. Verify that a unicast route is available between the two devices 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 switch are the same.

No SA entries in the switch 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 will be filtered off. No (S, G) entries of the local domain are advertised.
- If the **import-source** command is not executed, the system advertises all the (S, G) entries of the local domain. If MSDP fails to send (S, G) entries through SA messages, check whether the **import-source** command has been correctly configured.

Solution

1. Verify that a route is available between the devices. Use the **display ip routing-table** command to determine whether the unicast route between the devices is correct.
2. Verify that a unicast route is available between the two devices that will become MSDP peers.
3. Evaluate the configuration of the **import-source** command and its *acl-number* argument and be sure that the 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. Verify that a route is available between the devices. Use the **display ip routing-table** command to determine whether the unicast route between the devices is correct.
2. Verify that a unicast route is available between the two devices that will become MSDP peers.
3. Evaluate 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

This document covers configuration tasks related to multiprotocol BGP for IP multicast only. For more information about BGP, see *Layer 3—IP Routing Configuration Guide*.

For more information about RPF, see "Configuring multicast routing and forwarding."

MBGP overview

BGP-4 can carry routing information for IPv4 only. IETF defined MBGP extensions to carry routing information for multiple network layer protocols.

For a network, the multicast topology might be different from the unicast topology. To meet the requirement, the MBGP extensions enable BGP to carry the unicast NLRI and multicast NLRI separately, and the multicast NLRI performs RPF exclusively. In this way, route selection for a destination through the unicast routing table and through the multicast routing table will have different results, ensuring normal unicast and multicast routing.

MBGP is defined in RFC 2858 (Multiprotocol Extensions for BGP-4).

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*

Configuring MBGP basic functions

Prerequisites

Before configuring MBGP, make sure that neighboring nodes can access each other at the network layer.

Procedure

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Specify a peer or peer group and its AS number.	**peer** { *group-name* | *ip-address* } **as-number** *as-number*	Required. Not specified by default.
4. Enter IPv4 MBGP address family view.	**ipv4-family multicast**	Required.

To do...	Use the command...	Remarks
5. Enable a peer or peer group created in IPv4 unicast view.	**peer** { *group-name* | *ip-address* } **enable**	Required. Not enabled by default.
6. Specify a preferred value for routes from an IPv4 MBGP peer or peer group.	**peer** { *group-name* | *ip-address* } **preferred-value** *value*	Optional. The default preferred value is 0.

Controlling route advertisement and reception

Prerequisites

Configure MBGP basic functions before configuring this task.

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 learns the information by itself.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv4 MBGP address family view.	**ipv4-family multicast**	—
4. Enable route redistribution from another routing protocol.	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	At least one of these approaches is required. No route redistribution is configured by default. Currently, the **allow-direct** keyword is available only when the specified routing protocol is OSPF.
5. Inject a network into the MBGP routing table.	**network** *ip-address* [*mask* | *mask-length*] [**short-cut** | **route-policy** *route-policy-name*]	

The Origin attribute of routes redistributed into the MBGP routing table with the **import-route** command is Incomplete.

The Origin attribute of routes injected into the MBGP routing table with the **network** command is IGP.

The networks to be injected must exist in the local IP routing table, and using a routing policy makes route control more flexible.

Configure default route redistribution into MBGP

Using **import-route** cannot redistribute any default route into MBGP. This task allows you to do so.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—

To do...	Use the command...	Remarks
3. Enter MBGP address family view.	**ipv4-family multicast**	—
4. Enable route redistribution from another routing protocol.	**import-route** *protocol* [{ *process-id* | **all-processes** } [**allow-direct** | **med** *med-value* | **route-policy** *route-policy-name*] *]	Required. No route redistribution is configured by default. Currently, 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**	Required. Not enabled by default.

Configuring MBGP route summarization

To reduce the routing table size on medium and large MBGP networks, you must configure route summarization on peers. MBGP supports the following 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 by 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 do...		Use the command...	Remarks
1. Enter system view.		**system-view**	—
2. Enter BGP view.		**bgp** *as-number*	—
3. Enter IPv4 MBGP address family view.		**ipv4-family multicast**	—
4. Configure MBGP route summarization.	a. Enable automatic route summarization.	**summary automatic**	Required. No route summarization is configured by default. Choose either as needed. If both are configured, the manual route summarization takes effect.
	b. Configure manual route summarization.	**aggregate** *ip-address* { *mask* | *mask-length* } [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*] *	

Advertising a default route to an IPv4 MBGP peer or peer group

To do...	Use the command...	Remarks
1. Enter system view	**system-view**	—

To do...	Use the command...	Remarks
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv4 MBGP address family view.	**ipv4-family multicast**	—
4. Advertise a default route to an MBGP peer or peer group.	**peer** { *group-name* | *ip-address* } **default-route-advertise** [**route-policy** *route-policy-name*]	Required. 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 MBGP peer or peer group, regardless of whether the default route is available in the routing table.

Configuring outbound MBGP route filtering

If several filtering policies are configured, they are applied in the following sequence:

- **filter-policy export**
- **peer filter-policy export**
- **peer as-path-acl export**
- **peer ip-prefix export**
- **peer route-policy export**

Only the routes that have passed all the configured policies can be advertised.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv4 MBGP address family view.	**ipv4-family multicast**	—
4. Configure the filtering of redistributed routes.	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]	At least one of these approaches is required. No outbound route filtering is configured by default.
5. Apply a routing policy to advertisements to an IPv4 MBGP peer/peer group.	**peer** { *group-name* | *peer-address* } **route-policy** *route-policy-name* **export**	
6. Reference an ACL to filter advertisements to an IPv4 MBGP peer/peer group.	**peer** { *group-name* | *ip-address* } **filter-policy** *acl-number* **export**	
7. Reference an AS path ACL to filter route advertisements to an IPv4 MBGP peer/peer group.	**peer** { *group-name* | *ip-address* } **as-path-acl** *as-path-acl-number* **export**	
8. Reference an IP prefix list to filter route advertisements to an IPv4 MBGP peer/peer group.	**peer** { *group-name* | *ip-address* } **ip-prefix** *ip-prefix-name* **export**	

Configuring inbound MBGP route filtering

MBGP route reception filtering policies can filter out unqualified routes from an MBGP peer or 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 do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv4 MBGP address family view.	**ipv4-family multicast**	—
4. Filter incoming routes using an ACL or IP prefix list.	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**	At least one of these approaches is required. No inbound route filtering is configured by default.
5. Reference a routing policy to routes from an IPv4 MBGP peer/peer group.	**peer** { *group-name* | *ip-address* } **route-policy** *policy-name* **import**	
6. Reference an ACL to filter routing information from an IPv4 MBGP peer/peer group.	**peer** { *group-name* | *ip-address* } **filter-policy** *acl-number* **import**	
7. Reference an AS path ACL to filter routing information from an IPv4 MBGP peer/peer group.	**peer** { *group-name* | *ip-address* } **as-path-acl** *as-path-acl-number* **import**	
8. Reference an IP prefix list to filter routing information from an IPv4 MBGP peer/peer group.	**peer** { *group-name* | *ip-address* } **ip-prefix** *ip-prefix-name* **import**	
9. Specify the maximum number of routes that can be received from an IPv4 MBGP peer/peer group.	**peer** { *group-name* | *ip-address* } **route-limit** *limit* [*percentage*]	Optional. The number is unlimited by default.

Members of a peer group can have different route reception filtering policies from the peer group.

Configuring MBGP route dampening

By configuring MBGP route dampening, you can suppress

MBGP route dampening prevents unstable routes from being added to the MBGP routing table or being advertised to MBGP peers.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv4 MBGP address family view.	**ipv4-family multicast**	—
4. Configure BGP route dampening parameters.	**dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*] *	Required. Not configured by default.

Configuring MBGP route attributes

You can modify MBGP route attributes to affect route selection.

Prerequisites

Before configuring this task, configure MBGP basic functions.

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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv4 MBGP address family view.	**ipv4-family multicast**	—
4. Configure preferences for external, internal, local MBGP routes.	**preference** { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }	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

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv4 MBGP address family view.	**ipv4-family multicast**	—
4. Configure the default local preference.	**default local-preference** *value*	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 do…		Use the command…	Remarks
1. Enter system view.		**system-view**	—
2. Enter BGP view.		**bgp** *as-number*	—
3. Enter IPv4 MBGP address family view.		**ipv4-family multicast**	—
4. Configure the MED attribute.	a. Configure the default MED value.	**default med** *med-value*	Optional. Defaults to 0.
	b. Enable the comparison of the MED of routes from different Ass.	**compare-different-as-med**	Optional. Not enabled by default.
	c. Enable the comparison of the MED of routes from each AS.	**bestroute compare-med**	Optional. Not enabled by default.
	d. 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 switch as the next hop of routes sent to an MBGP iBGP peer or peer group. If load balancing is configured, the switch 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 third-party next-hop network, that is, when the local router has two multicast eBGP peers in a broadcast network, the router does not specify itself as the next hop of routing information sent to the eBGP peers unless the **peer next-hop-local** command is configured.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv4 MBGP address family view.	**ipv4-family multicast**	—

To do...	Use the command...	Remarks
4. Specify the router as the next hop of routes sent to a peer/peer group.	**peer** { *group-name* | *ip-address* } **next-hop-local**	Optional. By default, the next hop of routes sent to a MBGP eBGP peer/peer group is the advertising router, but that of routes sent to a MBGP iBGP peer/peer group is not.

Configuring the AS-PATH attribute

In general, MBGP checks whether the AS_PATH attribute of a route from a peer contains the local AS number. If yes, MBGP discards the route to avoid routing loops.

To do...		Use the command...	Remarks
1. Enter system view.		**system-view**	—
2. Enter BGP view.		**bgp** *as-number*	—
3. Enter IPv4 MBGP address family view.		**ipv4-family multicast**	—
4. Configure the AS_PATH attribute.	a. Specify the maximum number of times the local AS number can appear in routes from the peer/peer group.	**peer** { *group-name* | *ip-address* } **allow-as-loop** [*number*]	Optional. By default, the local AS number can not appear in routes from a peer/peer group.
	b. 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.
	c. Configure updates to a peer/peer group to not keep private AS numbers.	**peer** { *group-name* | *ip-address* } **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.

Prerequisites

Configure BGP basic functions before configuring this task.

Configuring MBGP soft reset

After modifying a route selection policy, you must 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.

If a peer that does not support route refresh exists in the network, you must use the **peer keep-all-routes** command to save all routes from the peer. When the routing policy is changed, the system will update the MBGP routing table and apply the new policy.

Soft reset through route-refresh

If the peer is enabled with route refresh, when the MBGP route selection policy is modified on a switch, the switch advertises a route-refresh message to its MBGP peers. The MBGP peers resend their routing information to the switch after they receive the message. Therefore, the local switch can perform dynamic route update and apply the new policy without terminating MBGP connections.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enable BGP route refresh for a peer/peer group.	**peer** { *group-name* | *ip-address* } **capability-advertise route-refresh**	Optional. Enabled by default.

Perform a manual soft reset

If the peer does not support route refresh, 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 do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Disable BGP route-refresh and multi-protocol extensions for a peer/peer group.	**peer** { *group-name* | *ip-address* } **capability-advertise conventional**	Optional. Enabled by default.
4. Enter IPv4 MBGP address family view.	**ipv4-family multicast**	—
5. Keep all original routes from a peer/peer group regardless of whether they pass the inbound filtering policies.	**peer** { *group-name* | *ip-address* } **keep-all-routes**	Required. Not kept by default.
6. Return to user view.	**return**	—
7. Soft-reset MBGP connections manually.	**refresh bgp ipv4 multicast** { **all** | *ip-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }	Optional.

Enabling the MBGP ORF capability

The BGP 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 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 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 9.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enable BGP route refresh for a peer/peer group.	**peer** { *group-name* | *ip-address* } **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 the *Layer 3—IP Routing Command Reference*.
4. Enable the non-standard ORF capability for a BGP peer/peer group.	**peer** { *group-name* | *ipv6-address* } **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 the *Layer 3—IP Routing Command Reference*.
5. Enter MBGP address family view.	**ipv4-family multicast**	—
6. Enable the ORF IP prefix negotiation capability for a BGP peer/peer group.	**peer** { *group-name* | *ip-address* } **capability-advertise orf ip-prefix** { **both** | **receive** | **send** }	Optional. Not supported by default.

Table 9 Description of the both, send, and receive parameters and the negotiation result

Local parameter	Peer parameter	Negotiation result
send	receive	The ORF sending capability is enabled locally and the ORF receiving capability is enabled on the peer.
	both	
receive	send	The ORF receiving capability is enabled locally and the ORF sending capability is enabled on the peer.
	both	
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

To do…	Use the command…	Remarks
1. Enter system view.	system-view	—
2. Enter BGP view.	**bgp** as-number	—
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	—
4. Configure the maximum number of MBGP routes for load balancing.	**balance** *number*	Required. Not configured by default.

Configuring a large scale MBGP network

Prerequisites

Before configuring this task, you need to 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.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Create a BGP peer group.	**group** *group-name* [**external** | **internal**]	Required. Not created by default.
4. Add a peer into the peer group.	**peer** *ip-address* **group** *group-name* [**as-number** *as-number*]	Required. No peer is added by default.
5. Enter IPv4 MBGP address family view.	**ipv4-family multicast**	—
6. Enable the IPv4 unicast peer group.	**peer** *group-name* **enable**	Required
7. Add an IPv4 MBGP peer to the peer group.	**peer** *ip-address* **group** *group-name*	Required Not configured by default.

To configure an MBGP peer group, you need to 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 need to add the corresponding IPv4 unicast peer to the IPv4 BGP peer group.

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, define extended community attributes as needed.

To do...		Use the command...	Remarks
1. Enter system view.		system-view	—
2. Enter BGP view.		**bgp** as-number	—
3. Enter IPv4 MBGP address family view.		ipv4-family multicast	—
4. Advertise the community attribute to an MBGP peer/peer group.	a. Advertise the community attribute to an MBGP peer/peer group.	**peer** { *group-name* | *ip-address* } **advertise-community**	Required. Not configured by default.
	b. Advertise the extended community attribute to an MBGP peer/peer group.	**peer** { *group-name* | *ip-address* } **advertise-ext-community**	
5. Apply a routing policy to routes advertised to an MBGP peer/peer group.		**peer** { group-name | ip-address } **route-policy** route-policy-name **export**	Required. Not configured by default.

When configuring MBGP community, you need to reference a routing policy to define the specific community attributes, and apply the routing policy for route advertisement.

For routing policy configuration, see *Routing Policy* in *Layer 3 – IP Routing Configuration Guide*.

Configuring an MBGP route reflector

To guarantee the connectivity between multicast iBGP peers in an AS, you must make them fully meshed. This becomes impractical when large numbers of multicast iBGP peers exist. Configuring route reflectors can solve this problem.

To do...	Use the command...	Remarks
1. Enter system view.	system-view	—
2. Enter BGP view.	**bgp** as-number	—
3. Enter IPv4 MBGP address family view.	ipv4-family multicast	—
4. Configure the router as a route reflector and specify an MBGP peer/peer group as its client.	**peer** { group-name | peer-address } **reflect-client**	Required. Not configured by default.
5. Enable route reflection between clients.	reflect between-clients	Optional. Enabled by default.

To do...	Use the command...	Remarks
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.

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 is used to identify 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.

Displaying and maintaining MBGP

To do...	Use the command...	Remarks
Display the IPv4 MBGP routing table.	**display ip multicast routing-table** [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the IPv4 MBGP routing information matching the specified destination IP address.	**display ip multicast routing-table** *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display MBGP peer group information.	**display bgp multicast group** [*group-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the advertised networks.	**display bgp multicast network** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display AS path information.	**display bgp multicast paths** [*as-regular-expression* | **|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display MBGP peer/peer group information.	**display bgp multicast peer** [[*ip-address*] **verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the prefix entries in the ORF information from the specified BGP peer.	**display bgp multicast peer** *ip-address* **received ip-prefix** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display MBGP routing information.	**display bgp multicast routing-table** [*ip-address* [{ *mask* | *mask-length* } [**longer-prefixes**]]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display MBGP routing information matching the AS path ACL.	**display bgp multicast routing-table as-path-acl** *as-path-acl-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display MBGP CIDR routing information.	**display bgp multicast routing-table cidr** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display MBGP routing information matching the specified BGP community.	**display bgp multicast routing-table community**[aa:nn&<1-13>] [**no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

To do…	Use the command…	Remarks
Display MBGP routing information matching an MBGP community list	**display bgp multicast routing-table community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16> [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display MBGP dampened routing information.	**display bgp multicast routing-table dampened** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display MBGP dampening parameter information.	**display bgp multicast routing-table dampening parameter** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display MBGP routing information originating from different Ass.	**display bgp multicast routing-table different-origin-as** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPv4 MBGP routing flap statistics.	**display bgp multicast routing-table flap-info** [**regular-expression** *as-regular-expression* | [**as-path-acl** *as-path-acl-number* | *ip-address* [{ *mask* | *mask-length* } [**longer-match**]]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]]	Available in any view.
Display IPv4 MBGP routing information sent to or received from an MBGP peer.	**display bgp multicast routing-table peer** *ip-address* { **advertised-routes** | **received-routes** } [*network-address* [*mask* | *mask-length*] | **statistic**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPv4 MBGP routing information matching an AS regular expression.	**display bgp multicast routing-table regular-expression** *as-regular-expression*	Available in any view.
Display IPv4 MBGP routing statistics.	**display bgp multicast routing-table statistic** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

Resetting MBGP connections

To do…	Use the command…	Remarks
Reset specified MBGP connections.	**reset bgp ipv4 multicast** { **all** | *as-number* | *ip-address* | **group** *group-name* | **external** | **internal** }	Available in user view.

Clearing MBGP information

To do…	Use the command…	Remarks
Clear dampened routing information and release suppressed routes.	**reset bgp ipv4 multicast dampening** [*ip-address* [*mask* | *mask-length*]]	Available in user view.
Clear MBGP route flap statistics.	**reset bgp ipv4 multicast flap-info** [**regexp** *as-path-regexp* | **as-path-acl** *as-path-acl-number* | *ip-address* [*mask* | *mask-length*]]	Available in user view.

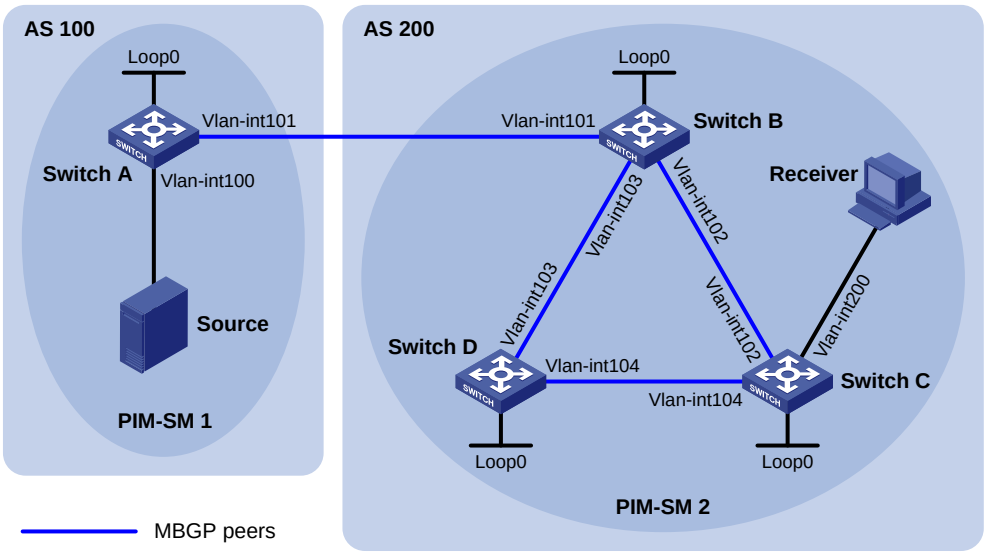
MBGP configuration example

Network requirements

As shown in Figure 63:

- 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 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 through MBGP between Router A and Router B.

Figure 63 Network diagram for MBGP configuration



Device	Interface	IP address	Device	Interface	IP address
Source	-	10.110.1.100/24	Switch C	Vlan-int200	10.110.2.1/24
Switch A	Vlan-int100	10.110.1.1/24		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		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		Loop0	4.4.4.4/32
	Loop0	2.2.2.2/32			

Procedure

1. Configure IP addresses for interfaces as shown in Figure 63 (detailed steps are not included here).
2. Configure OSPF (detailed steps are not included here).
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 **display bgp multicast peer** 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 **display msdp brief** to display MSDP peers on a switch. For example, display brief information about MSDP peers on Switch B.

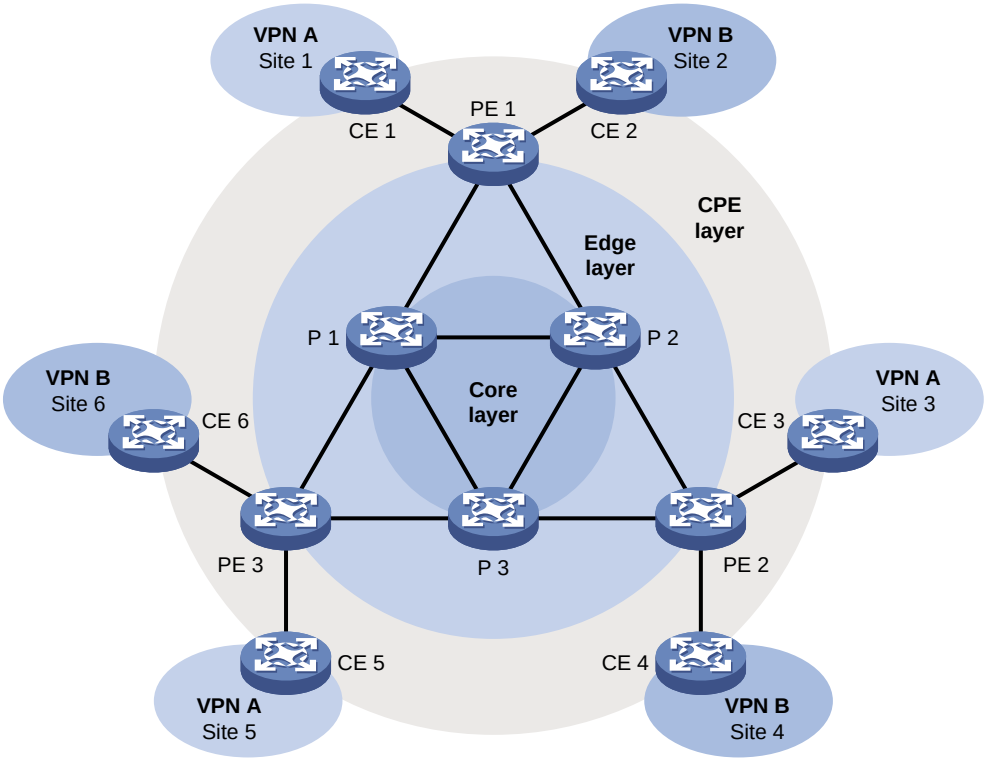
```
[SwitchB] display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
  Configured   Up           Listen       Connect      Shutdown     Down
  1            1            0            0            0            0
  Peer's Address    State    Up/Down time    AS     SA Count   Reset Count
  192.168.1.1       Up       00:07:17        100    1          0
```

Configuring multicast VPN

For details about MPLS L3VPN, see *MPLS Configuration Guide*. For details about BGP, see *Layer 3 – IP Routing Configuration Guide*.

Multicast VPN is a technique that implements multicast delivery in MPLS L3VPN networks. An MPLS L3VPN is a VPN implemented based on the extension technologies of BGP and MPLS. It comprises a set of customer sites that are interconnected only by means of an MPLS provider backbone network. You can think of The VPN as a set of policies that control the interconnections between these sites.

Figure 64 Typical application of MPLS L3VPNs



As shown in Figure 64, VPN A comprises Site 1, Site 3, and Site 5, and VPN B comprises Site 2, Site 4, and Site 6. A VPN involves the following types of devices:

- P device—Device in the core of the provider backbone network. A P device does not directly connect with CE devices, but it implements MPLS forwarding.
- PE device—Edge device in the provider backbone network. Directly connecting with one or more CE devices, a PE device processes VPN routing as a main MPLS L3VPN implementer.
- CE device—Edge device on a customer network. A CE device can be a router, a switch, or a host that implements route distribution on the customer network.

In an MPLS L3VPN environment, between any two sites that belong to the same VPN, packets are transmitted across the public network. The PE device at the entrance to the provider backbone attaches the following labels to the packets:

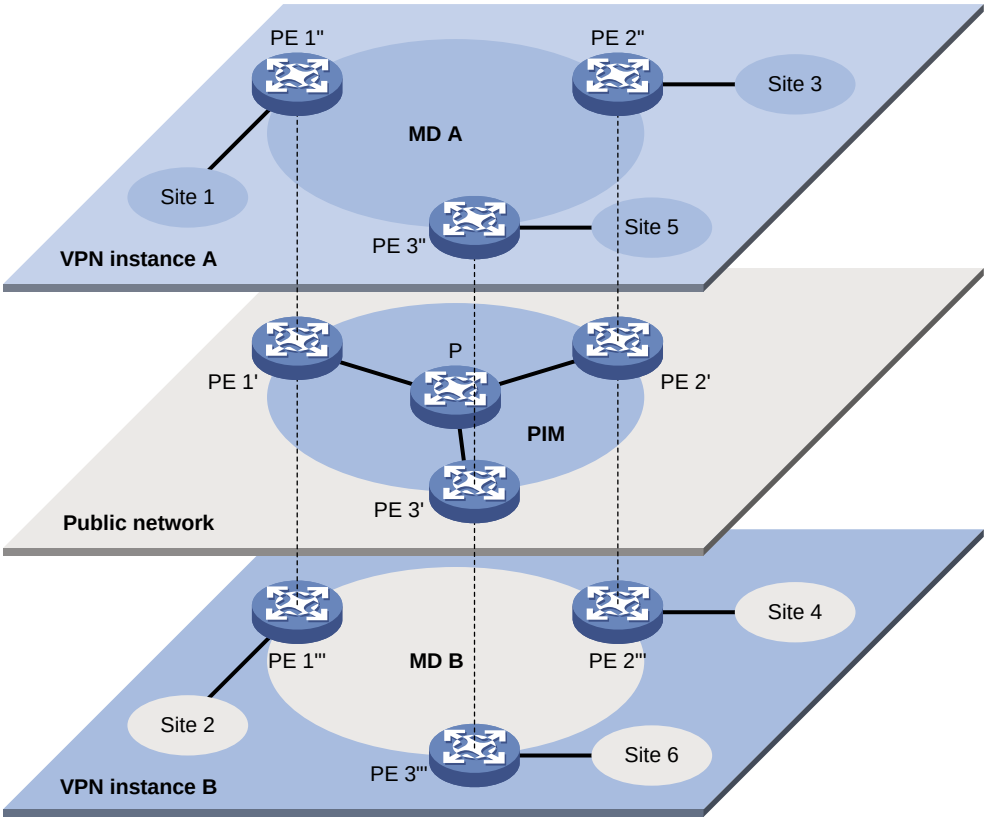
- Outer label—The outer label is used for switching within the backbone. It represents an LSP from the local PE to the peer PE. With this label, a packet can arrive to the peer PE along the LSP.
- Inner label—The inner label represents an LSP between two CE devices interconnected over the backbone network. It identifies the site to which the packet belongs. The PE forwards the packet to the target CE based on the inner label.

For more information about MPLS L3VPN, see the *MPLS Configuration Guide*. For more information about BGP, see the *Layer 3 – IP Routing Configuration Guide*.

Introduction to Multicast VPN

As shown in Figure 65, a network carries independent multicast services—the public network, VPN instance A, and VPN instance B. A PE multicast device at the edge of the public network supports multiple instances, equivalent to multiple independent multicast devices. Each instance corresponds to a plane, and all these planes are isolated from one another. For example, Figure 65 shows that the public network, VPN instance A and VPN instance B, are running on PE1. You can regard these instances as independent virtual devices, which are PE 1′, PE 1″, and PE 1‴. Each virtual device corresponds to a plane.

Figure 65 Multicast in multiple VPN instances



With multicast VPN, when a multicast source in VPN A sends a multicast stream to a multicast group, of all possible receivers on the network for that group, only those that belong to VPN A (in Site 1, Site 3, or Site 5) can receive the multicast stream. The stream is multicast in these sites and in the public network.

Prerequisites for implementing multicast VPN include:

- Support for VPN instance-based multicast within each site
- Support for public network based multicast within the public network

- PE devices that support multi-instance multicast:
  - Connecting with sites and supporting VPN instance based multicast
  - Connecting with the public network and supporting public network based multicast
  - Supporting information exchange and data conversion between the public network and the VPN instances

Introduction to MD-VPN

For details about the concepts of Protocol Independent Multicast (PIM), bootstrap router (BSR), candidate-BSR (C-BSR), rendezvous point (RP), candidate RP (C-RP), shortest path tree (SPT) and rendezvous point tree (RPT), see *PIM* in the *IP Multicast Configuration Guide*.

Comware implements multicast VPN by means of the multicast domain (MD) method. This multicast VPN implementation is referred to as MD-VPN.

The most significant advantage of MD-VPN is that it requires only the PE devices to support multiple instances. Multicast VPN can be implemented without upgrading any CE devices and P devices, and without changing the original PIM configuration of the CE devices and the P devices. In other words, the MD-VPN solution is transparent to the CE devices and the P devices.

Basic concepts in MD-VPN

Table 10 Basic concepts in MD-VPN

Concept	Description
Multicast domain (MD)	An MD is a set of VPN instances running on PE devices that can send multicast traffic to each other. Each MD uniquely corresponds to the same set of VPN instances.
Multicast distribution tree (MDT)	An MDT is a multicast distribution tree between all PE devices in the same VPN. Only share-MDT is available.
Multicast tunnel (MT)	An MT is a tunnel that interconnects all PEs in an MD for delivering VPN traffic within the MD.
Multicast tunnel interface (MTI)	An MTI is the entrance to or exit of an MT, equivalent to an entrance to or exit of an MD. PE devices use the MTI to access the MD. An MTI handles only multicast packets but not unicast packets. An MTI is automatically created with the configuration of a share-group and MTI binding for a VPN instance.
Share-group	In the public network, each MD is assigned an independent multicast address, called share-group. A share-group is the unique identifier of an MD in the public network. It helps build a share-MDT corresponding to the MD in the public network.
Share-multicast distribution tree (Share-MDT)	A share-MDT is an MDT that uses a share-group as its group address. In a VPN, the share-MDT is uniquely identified by the share-group. A share-MDT is automatically created after configuration and will always exist in the public network, regardless of the presence of any actual multicast services in the public network or the VPN.

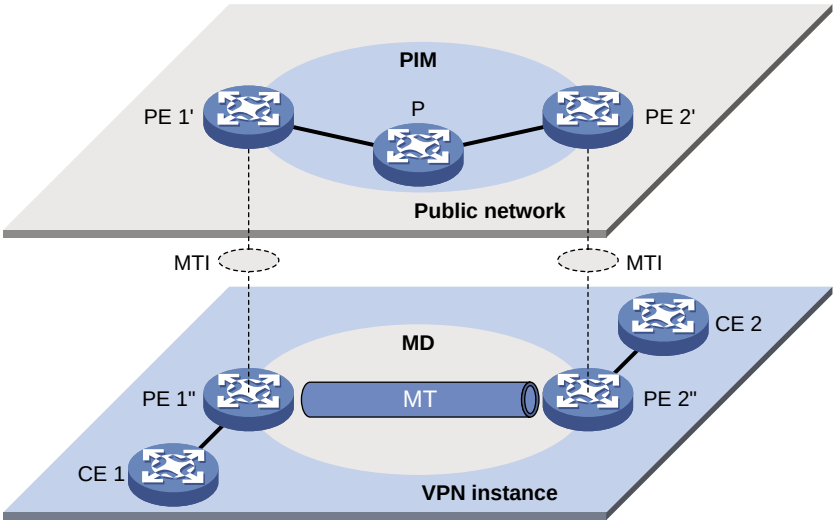
Implementation of MD-VPN

A VPN uniquely corresponds to an MD and an MD serves only one VPN, which is called a one-to-one relationship. Such a relationship exists between VPN, MD, MTI, and share-group.

Main points in the implementation of MD-VPN are as follows:

1. The public network of the service provider supports multicast. The PE devices must support the public network and multiple VPN instances. Each instance runs PIM independently. VPN multicast traffic between the PE devices and the CE devices is transmitted on a per-VPN-instance basis, and the public network multicast traffic between the PE devices and the P devices is transmitted through the public network.
2. Logically, an MD defines the transmission range of the multicast traffic of a specific VPN over the public network. Physically, an MD identifies all the PE devices that support that VPN in the public network. Different VPN instances correspond to different MDs. As shown in Figure 66, the ellipse area in the center of each VPN instance plane represents an MD, which serves that particular VPN. All the VPN multicast traffic in that VPN is transmitted within that MD.
3. Inside an MD, all the private traffic is transmitted through the MT. The local PE device encapsulates the VPN data into a public network packet, which is then forwarded in the public network, and the remote PE device decapsulates the packet to turn it back into a private packet.
4. The local PE device sends out VPN data through the MTI, and the remote PE devices receive the private data through the MTI. As shown in Figure 66, you can think of an MD as a private data transmission pool, and you can think of an MTI as an entrance or exit of the pool. The local PE device puts the private data into the transmission pool (the MD) through the entrance (MTI), and the transmission pool automatically duplicates the private data and transmits the data to each exit (MTI) of the transmission pool, so that any remote PE device that needs the data can get it from the respective exit (MTI).

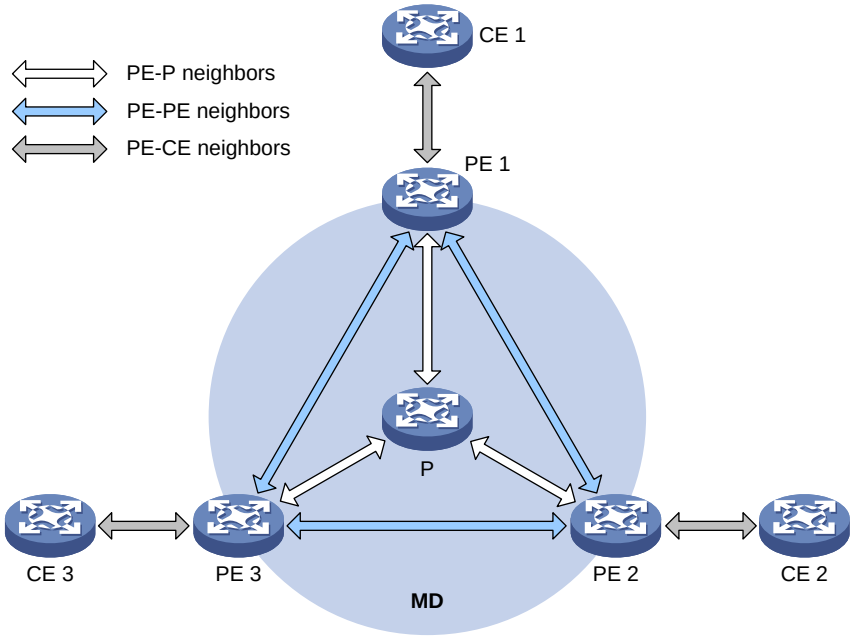
Figure 66 Relationship between PIM in the public network and an MD in a VPN instance



5. Each VPN instance receives a unique share-group address. The private network data is transparent to the public network. A PE device encapsulates any private network multicast packet within a normal public network multicast packet, no matter what multicast group the private network packet is destined for and whether it is a protocol packet or a data packet. The PE device uses the share-group as the public network multicast group for the packet. Then, the PE sends the public network multicast packet onto the public network.
6. A share-group corresponds to a unique MD. For each share-group, a unique share-MDT is constructed through the public network resources for multicast data forwarding. All the private network multicast packets transmitted in this VPN are forwarded along this share-MDT, no matter at which PE device they entered the public network.

PIM neighboring relationships in MD-VPN

Figure 67 PIM neighboring relationships in MD-VPN



PIM neighboring relationships are established between two or more directly interconnected devices on the same subnet. As shown in Figure 67, the types of PIM neighboring relationships in MD-VPN are as follows:

- PE-P neighboring relationship—PIM neighboring relationship established between the public network interface on a PE device and an interface on the P device across the link.
- PE-PE neighboring relationship—PIM neighboring relationship established after a VPN instance on a PE device receives a PIM hello from a VPN instance on a remote PE device through an MTI.
- PE-CE neighboring relationship—PIM neighboring relationship established between a VPN-instance-associated interface on a PE device and an interface on a peer CE device.

Protocols and standards

- RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*
- draft-rosen-vpn-mcast-08, *Multicast in MPLS/BGP IP VPNs*

Implementing MD-VPN

This section describes how the MD-VPN technology is implemented, including the construction of a share-MDT, delivery of multicast traffic based on the share-MDT, and implementation of multi-AS MD-VPN.

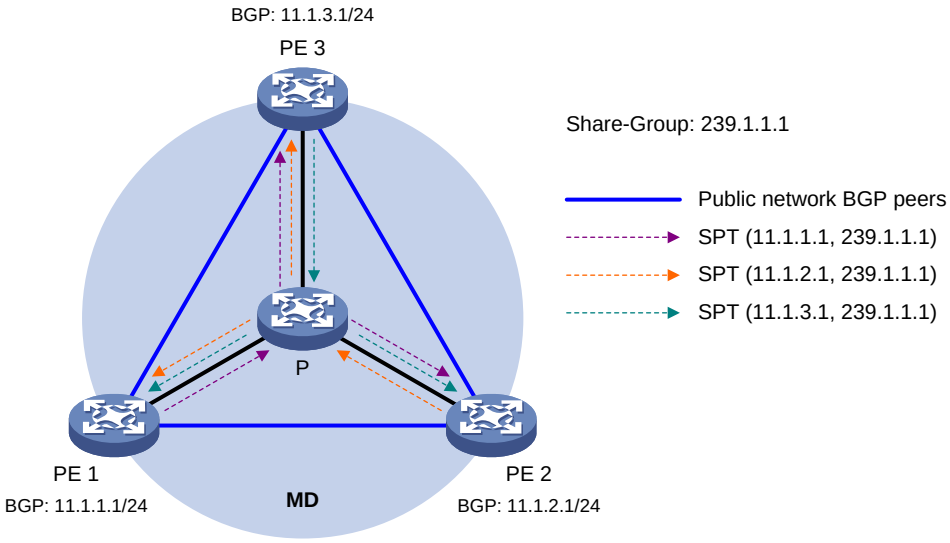
For a VPN instance, multicast data transmission in the public network is transparent. The MTIs at the local PE device and the remote PE device form a channel for the seamless transmission of VPN data over the public network. All that is known to the VPN instance is that the VPN data is sent out the MTI and then the remote site can receive the data through the MTI. Actually, the multicast data transmission process—the MDT transmission process—over the public network is very complicated.

Establishing share-MDT

The multicast routing protocol running in the public network can be PIM-DM or PIM-SM. The process of creating a share-MDT is different in these two PIM modes.

Establishing share-MDT in a PIM-DM network

Figure 68 Share-MDT establishment in a PIM-DM network



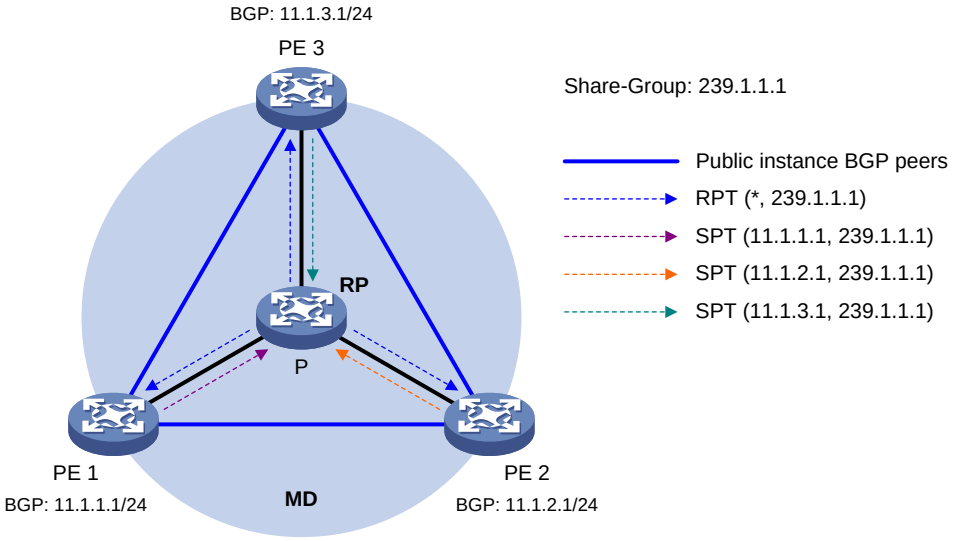
As shown in Figure 68, PIM-DM is enabled in the network and all the PE devices support VPN instance A. The process of establishing a share-MDT is as follows:

The public network on PE 1 initiates a flood-prune process in the entire public network, with the BGP interface address (the interface address used to establish the BGP peer) as the multicast source address and the share-group address as the multicast group address. All the other PE devices that are running VPN instance A are group members, so that a (11.1.1.1, 239.1.1.1) state entry is created on each device along the path in the public network. This forms an SPT with PE 1 as the root, and PE 2 and PE 3 as leaves.

At the same time, PE 2 and PE 3 respectively initiate a similar flood-prune process. Finally, three independent SPTs are established in the MD. In the PIM-DM network, these independent SPTs constitute a share-MDT.

Establishing share-MDT in a PIM-SM network

Figure 69 Share-MDT establishment in a PIM-SM network



As shown in Figure 69, PIM-SM is enabled in the network and all the PE devices support VPN instance A. The process of establishing a share-MDT is as follows:

1. The public instance on PE 1 initiates a join to the public network RP, with the share-group address as the multicast group address in the join message, and a (*, 239.1.1.1) state entry is created on each device along the path in the public network. At the same time, PE 2 and PE 3 respectively initiate a similar join process. Finally, an RPT is established in the MD, with the public network RP as the root and PE 1, PE 2, and PE 3 as leaves.
2. The public instance on PE 1 registers the multicast source with the public network RP and the public network RP initiates a join to PE 1. With the BGP interface address as the multicast source address and the share-group address as the multicast group address, a (11.1.1.1, 239.1.1.1) state entry is created on each device along the path in the public network. At the same time, PE 2 and PE 3 respectively initiate a similar register process. Finally, three SPTs between the PE devices and the RP are established in the MD.

In the PIM-SM network, the RPT (the (*, 239.1.1.1) tree, and the three independent SPTs) constitutes a share-MDT.

Share-MDT characteristics

A share-MDT is characterized as follows, no matter whether-DM or PIM-SM is running in the public network:

- All PE devices that support this VPN instance join the share-MDT.
- All VPN multicast packets that belong to this VPN, including protocol packets and data packets, are forwarded along the share-MDT to every PE device in the public network, even if they have no active receivers downstream.

Share-MDT-based delivery

A share-MDT can be used for delivering multicast packets, including both multicast protocol packets and multicast data packets. However, the transmission processes for these two types of multicast packets are different.

Delivering multicast protocol packets

To forward the multicast protocol packets of a VPN over the public network, the local PE device encapsulates them into public-network multicast data packets. These packets are transmitted along the share-MDT, and then decapsulated on the remote PE device to go into the normal protocol procedure. Finally a distribution tree is established across the public network. The following describes how multicast protocol packets are forwarded in the following circumstances:

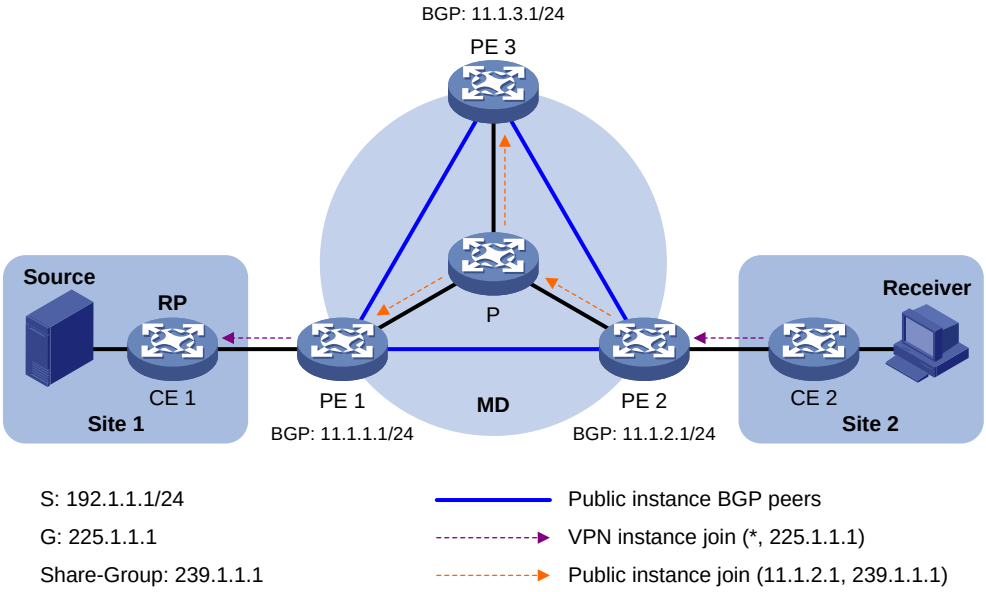
- If the VPN network runs PIM-DM:
  - Hello packets are forwarded among MTI interfaces to establish PIM neighboring relationships.
  - A flood-prune process (in PIM-DM) is initiated across the public network to establish an SPT across the public network.
- If the VPN network runs PIM-SM:
  - Hello packets are forwarded among MTI interfaces to establish PIM neighboring relationships.
  - If the receivers and the VPN RP are in different sites, a join process is initiated across the public network to establish an RPT.
  - If the multicast source and the VPN RP are in different sites, a registration process is initiated across the public network to establish an SPT.

All interfaces that belong to the same VPN, including those interfaces with VPN instance bindings and the MTI on PE devices, must run the same PIM mode.

The following example explains how multicast protocol packets are delivered based on the share-MDT while PIM-SM is running in both the public network and the VPNs network, with receivers and the VPN RP located in different sites.

As shown in Figure 70, PIM-SM is running in both the public network and the VPN network, Receiver for the VPN multicast group G (225.1.1.1) in Site 2 is attached to CE 2, and CE 1 of Site 1 acts as the RP for group G (225.1.1.1); the share-group address used to forward public network data is 239.1.1.1.

Figure 70 Transmission of multicast protocol packets



The work process of multicast protocol packets is as follows:

1. Receiver sends an IGMP membership report for multicast group G to CE 2. CE 2 creates a local (*, 225.1.1.1) state entry and sends a join message to the VPN RP (CE 1).

2. Upon receiving the join message from CE 2, the VPN instance on PE 2 creates a (*, 225.1.1.1) state entry with the upstream interface being the MTI, and then PE 2 processes the join message. Now, the VPN instance on PE 2 considers that the join message has been sent out the MTI.
3. PE 2 encapsulates the join message by means of Generic Routing Encapsulation (GRE), with its BGP interface address as the multicast source address and the share-group address as the multicast group address, to convert it into a normal, public network multicast data packet (11.1.2.1, 239.1.1.1), and then passes the packet to the public network on PE 2 to have it forwarded to the public network.
4. The multicast data packet (11.1.2.1, 239.1.1.1) is forwarded to the public network on all the PE devices along the share-MDT. Upon receiving this packet, every PE device decapsulates it to turn it back into a join message to be sent to the VPN RP. Then, each PE device checks the join message. If any PE device finds that the VPN RP is in the site it interfaces with, it passes the join message to the VPN instance on it. Otherwise, it discards the join message.
5. When receiving the join message, the VPN instance on PE 1 considers that it received the message from the MTI. PE 1 creates a local (*, 225.1.1.1) state entry, with the downstream interface being the MTI and the upstream interface being the one that leads to CE 1. At the same time, it sends a join message to CE 1, which is the VPN RP.
6. Upon receiving the join message from the VPN instance on PE 1, CE 1 creates a local (*, 225.1.1.1) state entry or updates the entry if it already exists. By now, the construction of an RPT across the public network is completed.

For details about GRE, see *Layer 3 – IP Services Configuration Guide*

Delivering multicast data packets

After the share-MDT is established, the multicast source forwards the VPN multicast data to the receivers in each site along the distribution tree. The VPN multicast packets are encapsulated into public network multicast packets on the local PE device, transmitted along the share-MDT, and then decapsulated on the remote PE device and transmitted in that VPN site. VPN multicast data flows are forwarded across the public network differently in the following two circumstances:

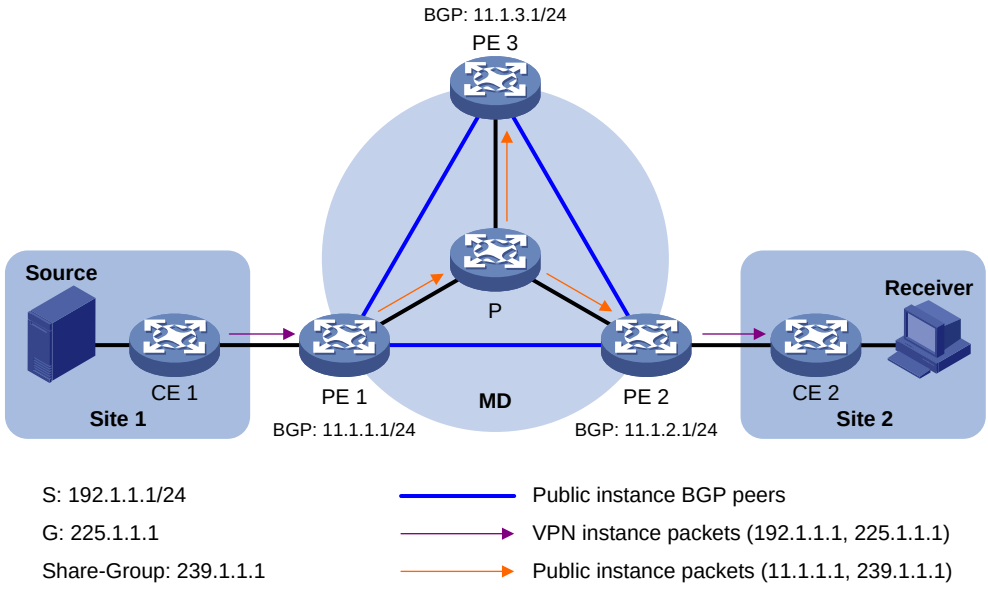
1. If PIM-DM is running in the VPN, the multicast source forwards multicast data to the receivers along the VPN SPT across the public network.
2. On a VPN running PIM-SM:
   - Before SPT switchover, if the multicast source and the VPN RP are in different sites, the multicast source forwards VPN multicast data to the VPN RP along the VPN SPT across the public network. If the VPN RP and the receiver are in different sites, the VPN RP forwards VPN multicast traffic to the receiver along the VPN RPT over the public network.
   - After SPT switchover, if the multicast source and the receiver are in different sites, the multicast source forwards VPN multicast data to the receiver along the VPN SPT across the public network.

For detailed description of RPT-to-SPT switchover, see *IP Multicast Configuration Guide*.

The following example explains how multicast data packets are delivered based on the share-MDT while PIM-DM is running in both the public network and the VPNs network.

As shown in Figure 71, PIM-DM is running in both the public network and the VPN sites, Receiver of the VPN multicast group G (225.1.1.1) in Site 2 is attached to CE 2, and Source in Site 1 sends multicast data to multicast group G); the share-group address used to forward public network multicast data is 239.1.1.1.

Figure 71 Delivery of multicast data packets



The VPN multicast traffic is delivered across the public network as follows.

3. Source sends customer multicast data (192.1.1.1, 225.1.1.1) to CE 1.
4. CE 1 forwards the VPN multicast data along an SPT to CE 1, and the VPN instance on PE 1 checks the MVRF. If the outgoing interface list of the forwarding entry contains an MTI, PE 1 processes the VPN multicast data. Now, the VPN instance on PE 1 considers that the VPN multicast data has been sent out the MTI.
5. PE 1 encapsulates the multicast data by means of GRE, with its BGP interface address as the multicast source address and the share-group address as the multicast group address, to convert it into a normal, public network multicast data packet (11.1.1.1, 239.1.1.1), and then passes the packet to the public network on PE 1 to have it forwarded to the public network.
6. The multicast data packet (11.1.1.1, 239.1.1.1) is forwarded to the public network on all the PE devices along the share-MDT. Upon receiving this packet, every PE device decapsulates it to turn it back into a VPN multicast data packet, and passes it to the corresponding VPN instance. If any PE has a downstream interface for an SPT, it forwards the VPN multicast packet down the SPT. Otherwise, it discards the packet.
7. The VPN instance on PE 2 searches the MVRF and finally delivers the VPN multicast data to Receiver. By now, the process of transmitting a VPN multicast packet across the public network is completed.

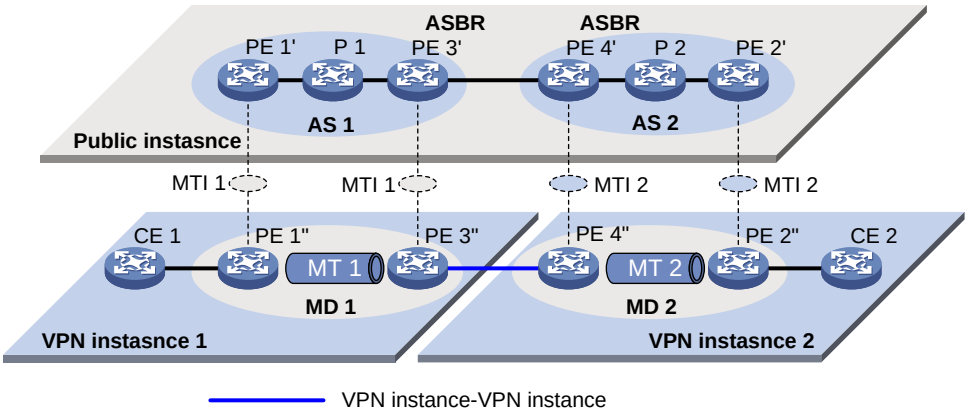
Multi-AS MD VPN

If nodes of a VPN network are allocated in multiple autonomous systems (ASs), these VPN nodes must be interconnected. To implement multi-AS VPN, VRF-to-VRF PE interconnectivity and multi-hop EBGP interconnectivity are available.

VRF-to-VRF PE interconnectivity

As shown in Figure 72, a VPN network involves two ASs, AS 1 and AS 2. PE 3 and PE 4 are the ASBR for AS 1 and AS 2 respectively. PE 3 and PE 4 are interconnected through their respective VPN instance and treat each other as a CE device.

Figure 72 VPN instance-VPN instance interconnectivity



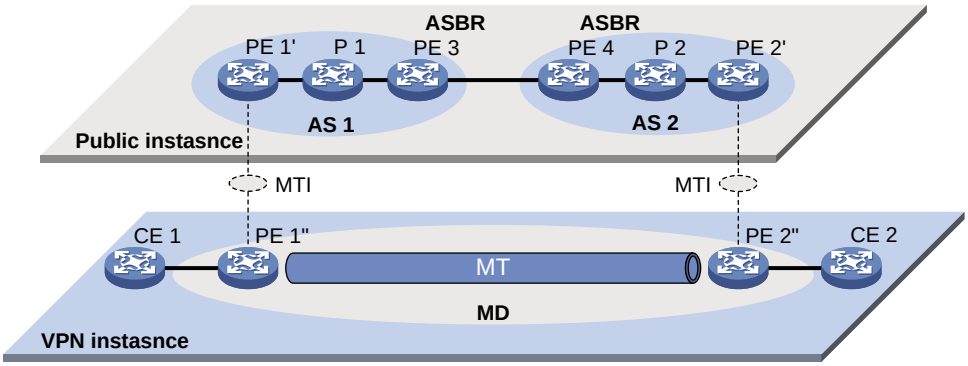
In the VPN instance–to–VPN instance interconnectivity approach, establish a separate MD within each AS so that VPN multicast traffic is transmitted between different ASs andbetween these MDs.

Because only VPN multicast traffic is forwarded between ASBRs, different PIM modes can run within different ASs. However, the same PIM mode (PIM-DM or PIM-SM) must run on all interfaces that belong to the same VPN (including interfaces with VPN bindings on ASBRs).

Multi-hop EBGP interconnectivity

As shown in Figure 73, a VPN network involves two ASs, AS 1 and AS 2. PE 3 and PE 4 are the ASBR for AS 1 and AS 2 respectively. PE 3 and PE 4 are interconnected through their respective public network instance and treat each other as a P device.

Figure 73 Multi-hop EBGP interconnectivity



In the multi-hop EBGP interconnectivity approach, only one MD needs to be established for all the ASs, and public network multicast traffic between different ASs is transmitted within this MD.

Configuring MD-VPN

Prerequisites

Before configuring MD-VPN, complete the following tasks:

- Configure any unicast routing protocol to provide intra-domain interoperability at the network layer.
- Configure MPLS L3VPN.
- Configure PIM (PIM-DM or PIM-SM).

- Determine the VPN instance names and route distinguishers (RDs)
- Determine the share-group addresses and an MTI numbers

Enabling IP multicast routing in a VPN instance

Before configuring any MD-VPN functionality for a VPN, you must enable IP multicast routing in the VPN instance.

To do...	Use the command...	Remarks
1. Enter system view	**system-view**	—
2. Create a VPN instance and enter VPN instance view.	**ip vpn-instance** *vpn-instance-name*	—
3. Configure an RD for the VPN instance.	**route-distinguisher** *route-distinguisher*	Required. No RD is configured for a VPN instance by default.
4. Enable IP multicast routing.	**multicast routing-enable**	Required. Defaults to disabled.

For details about the **ip vpn-instance** and **route-distinguisher** commands, see *MPLS Command Reference*.

For details about the **multicast routing-enable** command, see *IP Multicast Command Reference.*

Configuring a share-group and an MTI binding

By running multiple instances on each PE device, you enable the PE device to work for multiple VPNs. You must configure the same share-group address for the same VPN instance on different PE devices. With a share-group and an MTI number configured, the system automatically creates an MTI, binds the share-group address to the MTI, and binds the MTI to the current VPN instance.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VPN instance view.	**ip vpn-instance** *vpn-instance-name*	—
3. Configure a share-group address and an MTI binding.	**multicast-domain share-group** *group-address* **binding mtunnel** *mtunnel-number*	Required. No share-group address or MTI binding is configured.

After a BGP peer is configured with **peer connect-interface**, the MTI interface automatically obtains the **connect-interface** address and uses it as its own IP address. This IP address cannot be used in the VPNs network any more; Otherwise, the MTI interface will fail to obtain an IP address. When configuring multiple BGP peers on the same device, you must specify the same **connect-interface** address for these BGP peers; otherwise the MTI interface will also fail to obtain an IP address, either. For details about **peer connect-interface**, see *Layer 3 – IP Routing Command Reference*.

The MTI interface becomes up only after it obtains an IP address. On A5800&A5820X, in addition, you need first to use **service-loopback group** to configure a **multicast-tunnel** type service loopback group before an MTI interface can be brought up. For details about **service-loopback group**, see *Layer 2 – LAN Switching Command Reference*.

PIM on the MTI interface takes effect only after PIM is enabled on at least one interface of the VPN instance; when PIM is disabled on all the interfaces of the VPN instance, PIM on the MTI interface is disabled simultaneously.

Displaying and maintaining multicast VPN

To do...	Use the command...	Remarks
View the share-group information of the specified VPN instance in the MD.	**display multicast-domain vpn-instance** *vpn-instance-name* **share-group** { **local** | **remote** }	Available in any view.

Multicast VPN configuration examples

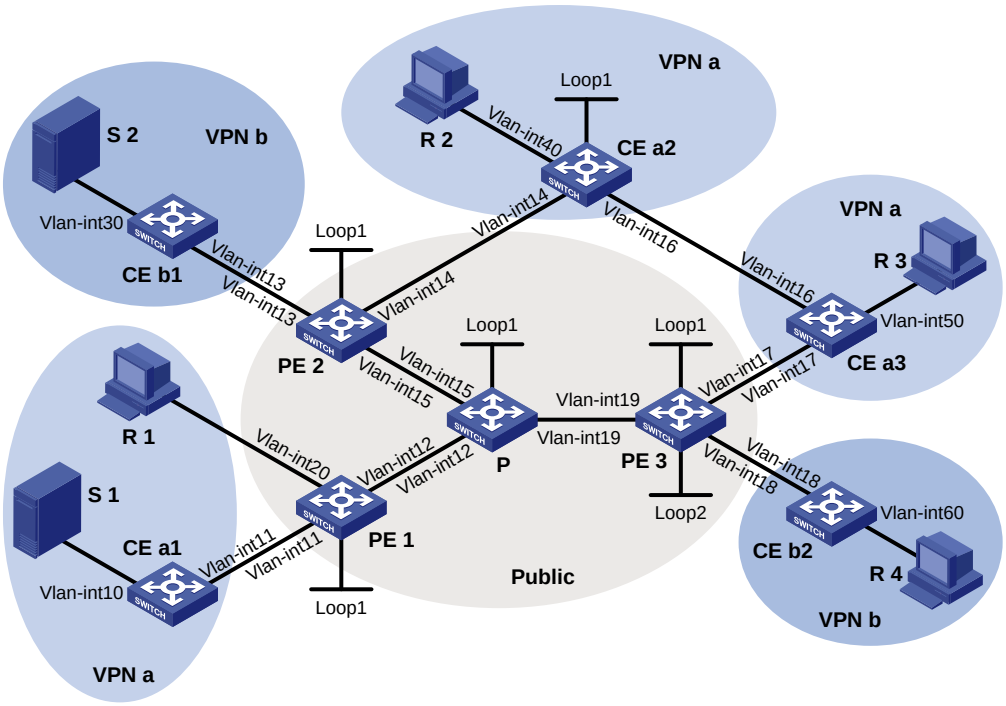
Single-AS MD VPN configuration

Network requirements

Item	Network requirements
Multicast sources and receivers	• In VPN a, S 1 is a multicast source, and R 1, R 2 and R3 are receivers. • In VPN b, S 2 is a multicast source, and R 4 is a receiver. • For VPN a, the share-group address is 239.1.1.1. • For VPN b, the share-group address is 239.2.2.2.
PE interfaces and VPN instances they belong to	• PE 1—VLAN-interface 11 and VLAN-interface 20 belong to VPN instance a; VLAN-interface 12 and Loopback 1 belong to the public network instance. • PE 2—VLAN-interface 13 belongs to VPN instance b; VLAN-interface 14 belongs to VPN instance a; VLAN-interface 15 and Loopback 1 belong to the public network instance. • PE 3—VLAN-interface 17 belongs to VPN instance a; VLAN-interface 18 and Loopback 2 belong to VPN instance b; VLAN-interface 19 and Loopback 1 belong to the public network instance.
Unicast routing protocols and MPLS	• Configure OSPF in the public network, and configure RIP between the PEs and CEs. • Establish BGP peer connections between PE 1, PE 2 and PE 3 on their respective Loopback 1 interface and exchange all VPN routes between them. • Configure MPLS in the public network.
IP multicast routing	• Enable IP multicast routing on the P device. • Enable IP multicast routing on the public network on PE 1, PE 2, and PE 3. • Enable IP multicast routing in VPN instance a on PE 1, PE 2, and PE 3. • Enable IP multicast routing in VPN instance b on PE 2 and PE 3. • Enable IP multicast routing on CE a1, CE a2, CE a3, CE b1, and CE b2.
IGMP	• Run IGMPv2 on VLAN-interface 20 of PE 1. • Run IGMPv2 on VLAN-interface 40 of CE a2, VLAN-interface 50 of CE a3, and VLAN-interface 60 of CE b2.

Item	Network requirements
PIM	• Enable PIM-SM on all interfaces of the P device. • Enable PIM-SM on all public and private network interfaces of PE 1, PE 2 and PE 3. • Enable PIM-SM on all interfaces of CE a1, CE a2, CE a3, CE b1, and CE b2. • Configure Loopback 1 of P as a C-BSR and a C-RP for the public network (to work for all multicast groups). • Configure Loopback 1 of CE a2 as a C-BSR and a C-RP for VPN a (to work for all multicast groups). • Configure Loopback 2 of PE 3 as a C-BSR and a C-RP for VPN b (to work for all multicast groups).

Figure 74 Network diagram for single-AS MD VPN configuration



Device	Interface	IP address	Device	Interface	IP address
S 1	—	10.110.7.2/24	PE 3	Vlan-int19	192.168.8.1/24
S 2	—	10.110.8.2/24		Vlan-int17	10.110.5.1/24
R 1	—	10.110.1.2/24		Vlan-int18	10.110.6.1/24
R 2	—	10.110.9.2/24		Loop1	1.1.1.3/32
R 3	—	10.110.10.2/24		Loop2	33.33.33.33/32
R 4	—	10.110.11.2/24	CE a1	Vlan-int10	10.110.7.1/24
P	Vlan-int12	192.168.6.2/24		Vlan-int11	10.110.2.2/24
	Vlan-int15	192.168.7.2/24	CE a2	Vlan-int40	10.110.9.1/24
	Vlan-int19	192.168.8.2/24		Vlan-int14	10.110.4.2/24
	Loop1	2.2.2.2/32		Vlan-int16	10.110.12.1/24

Device	Interface	IP address	Device	Interface	IP address
PE 1	Vlan-int12	192.168.6.1/24		Loop1	22.22.22.22/32
	Vlan-int20	10.110.1.1/24	CE a3	Vlan-int50	10.110.10.1/24
	Vlan-int11	10.110.2.1/24		Vlan-int17	10.110.5.2/24
	Loop1	1.1.1.1/32		Vlan-int16	10.110.12.2/24
PE 2	Vlan-int15	192.168.7.1/24	CE b1	Vlan-int30	10.110.8.1/24
	Vlan-int13	10.110.3.1/24		Vlan-int13	10.110.3.2/24
	Vlan-int14	10.110.4.1/24	CE b2	Vlan-int60	10.110.11.1/24
	Loop1	1.1.1.2/32		Vlan-int18	10.110.6.2/24

Procedure

1. Configure PE 1

Configure a Router ID, enable IP multicast routing on the public network, configure an MPLS LSR ID, and enable the LDP capability.

```
<PE1> system-view
[PE1] router id 1.1.1.1
[PE1] multicast routing-enable
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
```

Create VPN instance a, configure a RD for it, and create an egress route and an ingress route for it.

```
[PE1] ip vpn-instance a
[PE1-vpn-instance-a] route-distinguisher 100:1
[PE1-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE1-vpn-instance-a] vpn-target 100:1 import-extcommunity
```

Enable IP multicast routing in VPN instance a, configure a share-group address, and associate an MTI with the VPN instance.

```
[PE1-vpn-instance-a] multicast routing-enable
[PE1-vpn-instance-a] multicast-domain share-group 239.1.1.1 binding mtunnel 0
[PE1-vpn-instance-a] quit
```

Configure an IP address, and enable PIM-SM and LDP capability on the public network interface VLAN-interface 12.

```
[PE1] interface vlan-interface 12
[PE1-Vlan-interface12] ip address 192.168.6.1 24
[PE1-Vlan-interface12] pim sm
[PE1-Vlan-interface12] mpls
[PE1-Vlan-interface12] mpls ldp
[PE1-Vlan-interface12] quit
```

Bind VLAN-interface 20 to VPN instance a, configure an IP address and enable IGMP and PIM-SM on the interface.

```
[PE1] interface vlan-interface 20
```

```
[PE1-Vlan-interface20] ip binding vpn-instance a
[PE1-Vlan-interface20] ip address 10.110.1.1 24
[PE1-Vlan-interface20] igmp enable
[PE1-Vlan-interface20] pim sm
[PE1-Vlan-interface20] quit
```

Bind VLAN-interface 11 to VPN instance a, configure an IP address and enable PIM-SM on the interface.

```
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] ip binding vpn-instance a
[PE1-Vlan-interface11] ip address 10.110.2.1 24
[PE1-Vlan-interface11] pim sm
[PE1-Vlan-interface11] quit
```

Configure an IP address for Loopback 1, and enable PIM-SM.

```
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.1 32
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

Configure BGP.

```
[PE1] bgp 100
[PE1-bgp] group vpn-g internal
[PE1-bgp] peer vpn-g connect-interface loopback 1
[PE1-bgp] peer 1.1.1.2 group vpn-g
[PE1-bgp] peer 1.1.1.3 group vpn-g
[PE1-bgp] ipv4-family vpn-instance a
[PE1-bgp-a] import-route rip 2
[PE1-bgp-a] import-route direct
[PE1-bgp-a] quit
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer vpn-g enable
[PE1-bgp-af-vpnv4] peer 1.1.1.2 group vpn-g
[PE1-bgp-af-vpnv4] peer 1.1.1.3 group vpn-g
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```

With BGP peers configured on PE 1, the interfaces MTI 0 will automatically obtain an IP address, which is the loopback interface address specified in the BGP peer configuration. The PIM mode running on MTI 0 is the same as on the interfaces in VPN instance a.

Configure OSPF.

```
[PE1] ospf 1
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

Configure RIP

```
[PE1] rip 2 vpn-instance a
[PE1-rip-2] network 10.0.0.0
```

```
[PE1-rip-2] import-route bgp
[PE1-rip-2] return
```

2. Configure PE 2

Configure a Router ID, enable IP multicast routing on the public network, configure an MPLS LSR ID, and enable the LDP capability.

```
<PE2> system-view
[PE2] router id 1.1.1.2
[PE2] multicast routing-enable
[PE2] mpls lsr-id 1.1.1.2
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
```

Create VPN instance b, configure a RD for it, and create an egress route and an ingress route for it.

```
[PE2] ip vpn-instance b
[PE2-vpn-instance-b] route-distinguisher 200:1
[PE2-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE2-vpn-instance-b] vpn-target 200:1 import-extcommunity
```

Enable IP multicast routing in VPN instance b, configure a share-group address, and associate an MTI with the VPN instance.

```
[PE2-vpn-instance-b] multicast routing-enable
[PE2-vpn-instance-b] multicast-domain share-group 239.2.2.2 binding mtunnel 1
[PE2-vpn-instance-b] quit
```

Create VPN instance a, configure a RD for it, and create an egress route and an ingress route for it.

```
[PE2] ip vpn-instance a
[PE2-vpn-instance-a] route-distinguisher 100:1
[PE2-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE2-vpn-instance-a] vpn-target 100:1 import-extcommunity
```

Enable IP multicast routing in VPN instance a, configure a share-group address, and associate an MTI with the VPN instance.

```
[PE2-vpn-instance-a] multicast routing-enable
[PE2-vpn-instance-a] multicast-domain share-group 239.1.1.1 binding mtunnel 0
[PE2-vpn-instance-a] quit
```

Configure an IP address, and enable PIM-SM and LDP capability on the public network interface VLAN-interface 15.

```
[PE2] interface vlan-interface 15
[PE2-Vlan-interface15] ip address 192.168.7.1 24
[PE2-Vlan-interface15] pim sm
[PE2-Vlan-interface15] mpls
[PE2-Vlan-interface15] mpls ldp
[PE2-Vlan-interface15] quit
```

Bind VLAN-interface 13 to VPN instance b, configure an IP address and enable PIM-SM on the interface.

```
[PE2] interface vlan-interface 13
[PE2-Vlan-interface13] ip binding vpn-instance b
[PE2-Vlan-interface13] ip address 10.110.3.1 24
```

```
[PE2-Vlan-interface13] pim sm
[PE2-Vlan-interface13] quit
```

Bind VLAN-interface 14 to VPN instance a, configure an IP address and enable PIM-SM on the interface.

```
[PE2] interface vlan-interface 14
[PE2-Vlan-interface14] ip binding vpn-instance a
[PE2-Vlan-interface14] ip address 10.110.4.1 24
[PE2-Vlan-interface14] pim sm
[PE2-Vlan-interface14] quit
```

Configure an IP address for Loopback 1, and enable PIM-SM.

```
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 1.1.1.2 32
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```

Configure BGP.

```
[PE2] bgp 100
[PE2-bgp] group vpn-g internal
[PE2-bgp] peer vpn-g connect-interface loopback 1
[PE2-bgp] peer 1.1.1.1 group vpn-g
[PE2-bgp] peer 1.1.1.3 group vpn-g
[PE2-bgp] ipv4-family vpn-instance a
[PE2-bgp-a] import-route rip 2
[PE2-bgp-a] import-route direct
[PE2-bgp-a] quit
[PE2-bgp] ipv4-family vpn-instance b
[PE2-bgp-b] import-route rip 3
[PE2-bgp-b] import-route direct
[PE2-bgp-b] quit
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer vpn-g enable
[PE2-bgp-af-vpnv4] peer 1.1.1.1 group vpn-g
[PE2-bgp-af-vpnv4] peer 1.1.1.3 group vpn-g
[PE2-bgp-af-vpnv4] quit
[PE2-bgp] quit
```

With BGP peers configured on PE 2, the interfaces MTI 0 and MTI 1 will automatically obtain IP addresses, which are the loopback interface addresses specified in the BGP peer configuration. The PIM mode running on MTI 0 is the same as on the interfaces in VPN instance a, and the PIM mode running on MTI 1 is the same as on the interfaces in VPN instance b.

Configure OSPF.

```
[PE2] ospf 1
[PE2-ospf-1] area 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 1.1.1.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Configure RIP

```
[PE2] rip 2 vpn-instance a
[PE2-rip-2] network 10.0.0.0
[PE2-rip-2] import-route bgp
[PE2-rip-2] quit
[PE2] rip 3 vpn-instance b
[PE2-rip-3] network 10.0.0.0
[PE2-rip-3] import-route bgp
[PE2-rip-3] return
```

3. Configure PE 3

Configure a Router ID, enable IP multicast routing on the public network, configure an MPLS LSR ID, and enable the LDP capability.

```
<PE3> system-view
[PE3] router id 1.1.1.3
[PE3] multicast routing-enable
[PE3] mpls lsr-id 1.1.1.3
[PE3] mpls
[PE3-mpls] quit
[PE3] mpls ldp
[PE3-mpls-ldp] quit
```

Create VPN instance a, configure a RD for it, and create an egress route and an ingress route for it.

```
[PE3] ip vpn-instance a
[PE3-vpn-instance-a] route-distinguisher 100:1
[PE3-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE3-vpn-instance-a] vpn-target 100:1 import-extcommunity
```

Enable IP multicast routing in VPN instance a, configure a share-group address, and associate an MTI with the VPN instance.

```
[PE3-vpn-instance-a] multicast routing-enable
[PE3-vpn-instance-a] multicast-domain share-group 239.1.1.1 binding mtunnel 0
[PE3-vpn-instance-a] quit
```

Create VPN instance b, configure a RD for it, and create an egress route and an ingress route for it.

```
[PE3] ip vpn-instance b
[PE3-vpn-instance-b] route-distinguisher 200:1
[PE3-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE3-vpn-instance-b] vpn-target 200:1 import-extcommunity
```

Enable IP multicast routing in VPN instance b, configure a share-group address, and associate an MTI with the VPN instance.

```
[PE3-vpn-instance-b] multicast routing-enable
[PE3-vpn-instance-b] multicast-domain share-group 239.2.2.2 binding mtunnel 1
[PE3-vpn-instance-b] quit
```

Configure an IP address, and enable PIM-SM and LDP capability on the public network interface VLAN-interface 19.

```
[PE3] interface vlan-interface 19
[PE3-Vlan-interface19] ip address 192.168.8.1 24
[PE3-Vlan-interface19] pim sm
[PE3-Vlan-interface19] mpls
[PE3-Vlan-interface19] mpls ldp
```

```
[PE3-Vlan-interface19] quit
```

Bind VLAN-interface 17 to VPN instance a, configure an IP address and enable PIM-SM on the interface.

```
[PE3] interface vlan-interface 17
[PE3-Vlan-interface17] ip binding vpn-instance a
[PE3-Vlan-interface17] ip address 10.110.5.1 24
[PE3-Vlan-interface17] pim sm
[PE3-Vlan-interface17] quit
```

Bind VLAN-interface 18 to VPN instance b, configure an IP address and enable PIM-SM on the interface.

```
[PE3] interface vlan-interface 18
[PE3-Vlan-interface18] ip binding vpn-instance b
[PE3-Vlan-interface18] ip address 10.110.6.1 24
[PE3-Vlan-interface18] pim sm
[PE3-Vlan-interface18] quit
```

Configure an IP address for Loopback 1, and enable PIM-SM.

```
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 1.1.1.3 32
[PE3-LoopBack1] pim sm
[PE3-LoopBack1] quit
```

Bind Loopback 2 to VPN instance b, configure an IP address and enable PIM-SM on the interface.

```
[PE3] interface loopback 2
[PE3-LoopBack2] ip binding vpn-instance b
[PE3-LoopBack2] ip address 33.33.33.33 32
[PE3-LoopBack2] pim sm
[PE3-LoopBack2] quit
```

Configure Loopback 2 as a C-BSR and a C-RP for VPN b.

```
[PE3] pim vpn-instance b
[PE3-pim-b] c-bsr loopback 2
[PE3-pim-b] c-rp loopback 2
[PE3-pim-b] quit
```

Configure BGP.

```
[PE3] bgp 100
[PE3-bgp] group vpn-g internal
[PE3-bgp] peer vpn-g connect-interface loopback 1
[PE3-bgp] peer 1.1.1.1 group vpn-g
[PE3-bgp] peer 1.1.1.2 group vpn-g
[PE3-bgp] ipv4-family vpn-instance a
[PE3-bgp-a] import-route rip 2
[PE3-bgp-a] import-route direct
[PE3-bgp-a] quit
[PE3-bgp] ipv4-family vpn-instance b
[PE3-bgp-b] import-route rip 3
[PE3-bgp-b] import-route direct
[PE3-bgp-b] quit
[PE3-bgp] ipv4-family vpnv4
```

```
[PE3-bgp-af-vpnv4] peer vpn-g enable
[PE3-bgp-af-vpnv4] peer 1.1.1.1 group vpn-g
[PE3-bgp-af-vpnv4] peer 1.1.1.2 group vpn-g
[PE3-bgp-af-vpnv4] quit
[PE3-bgp] quit
```

With BGP peers configured on PE 3, the interfaces MTI 0 and MTI 1 will automatically obtain IP addresses, which are the loopback interface addresses specified in the BGP peer configuration. The PIM mode running on MTI 0 is the same as on the interfaces in VPN instance a, and the PIM mode running on MTI 1 is the same as on the interfaces in VPN instance b.

Configure OSPF.

```
[PE3] ospf 1
[PE3-ospf-1] area 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 1.1.1.3 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

Configure RIP

```
[PE3] rip 2 vpn-instance a
[PE3-rip-2] network 10.0.0.0
[PE3-rip-2] import-route bgp
[PE3-rip-2] quit
[PE3] rip 3 vpn-instance b
[PE3-rip-3] network 10.0.0.0
[PE3-rip-3] network 33.0.0.0
[PE3-rip-3] import-route bgp
[PE3-rip-3] return
```

4. Configure P:

Enable IP multicast routing on the public network, configure an MPLS LSR ID, and enable the LDP capability.

```
<P> system-view
[P] multicast routing-enable
[P] mpls lsr-id 2.2.2.2
[P] mpls
[P-mpls] quit
[P] mpls ldp
[P-mpls-ldp] quit
```

Configure an IP address, and enable PIM-SM and LDP capability on the public network interface VLAN-interface 12.

```
[P] interface vlan-interface 12
[P-Vlan-interface12] ip address 192.168.6.2 24
[P-Vlan-interface12] pim sm
[P-Vlan-interface12] mpls
[P-Vlan-interface12] mpls ldp
[P-Vlan-interface12] quit
```

Configure an IP address, and enable PIM-SM and LDP capability on the public network interface VLAN-interface 15.

```
[P] interface vlan-interface 15
[P-Vlan-interface15] ip address 192.168.7.2 24
[P-Vlan-interface15] pim sm
[P-Vlan-interface15] mpls
[P-Vlan-interface15] mpls ldp
[P-Vlan-interface15] quit
```

Configure an IP address, and enable PIM-SM and LDP capability on the public network interface VLAN-interface 19.

```
[P] interface vlan-interface 19
[P-Vlan-interface19] ip address 192.168.8.2 24
[P-Vlan-interface19] pim sm
[P-Vlan-interface19] mpls
[P-Vlan-interface19] mpls ldp
[P-Vlan-interface19] quit
```

Configure an IP address for Loopback 1, and enable PIM-SM.

```
[P] interface loopback 1
[P-LoopBack1] ip address 2.2.2.2 32
[P-LoopBack1] pim sm
[P-LoopBack1] quit
```

Configure Loopback 1 as a C-BSR and a C-RP for the public network instance.

```
[P] pim
[P-pim] c-bsr loopback 1
[P-pim] c-rp loopback 1
[P-pim] quit
```

Configure OSPF.

```
[P] ospf 1
[P-ospf-1] area 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
```

5. Configure CE a1.

Enable IP multicast routing.

```
<CEa1> system-view
[CEa1] multicast routing-enable
```

Configure an IP address for VLAN-interface 10 and enable PIM-SM on the interface.

```
[CEa1] interface vlan-interface 10
[CEa1-Vlan-interface10] ip address 10.110.7.1 24
[CEa1-Vlan-interface10] pim sm
[CEa1-Vlan-interface10] quit
```

Configure an IP address for VLAN-interface 11 and enable PIM-SM on the interface.

```
[CEa1] interface vlan-interface 11
[CEa1-Vlan-interface11] ip address 10.110.2.2 24
[CEa1-Vlan-interface11] pim sm
[CEa1-Vlan-interface11] quit
```

Configure RIP

```
[CEa1] rip 2
```

```
[CEa1-rip-2] network 10.0.0.0
```

6. Configure CE b1.

Enable IP multicast routing.

```
<CEb1> system-view
[CEb1] multicast routing-enable
```

Configure an IP address for VLAN-interface 30 and enable PIM-SM on the interface.

```
[CEb1] interface vlan-interface 30
[CEb1-Vlan-interface30] ip address 10.110.8.1 24
[CEb1-Vlan-interface30] pim sm
[CEb1-Vlan-interface30] quit
```

Configure an IP address for VLAN-interface 13 and enable PIM-SM on the interface.

```
[CEb1] interface vlan-interface 13
[CEb1-Vlan-interface13] ip address 10.110.3.2 24
[CEb1-Vlan-interface13] pim sm
[CEb1-Vlan-interface13] quit
```

Configure RIP

```
[CEb1] rip 3
[CEb1-rip-3] network 10.0.0.0
```

7. Configure CE a2.

Enable IP multicast routing.

```
<CEa2> system-view
[CEa2] multicast routing-enable
```

Configure an IP address for VLAN-interface 40 and enable IGMP and PIM-SM on the interface.

```
[CEa2] interface vlan-interface 40
[CEa2-Vlan-interface40] ip address 10.110.9.1 24
[CEa2-Vlan-interface40] igmp enable
[CEa2-Vlan-interface40] pim sm
[CEa2-Vlan-interface40] quit
```

Configure an IP address for VLAN-interface 14 and enable PIM-SM on the interface.

```
[CEa2] interface vlan-interface 14
[CEa2-Vlan-interface14] ip address 10.110.4.2 24
[CEa2-Vlan-interface14] pim sm
[CEa2-Vlan-interface14] quit
```

Configure an IP address for VLAN-interface 16 and enable PIM-SM on the interface.

```
[CEa2] interface vlan-interface 16
[CEa2-Vlan-interface16] ip address 10.110.12.1 24
[CEa2-Vlan-interface16] pim sm
[CEa2-Vlan-interface16] quit
```

Configure an IP address for Loopback 1, and enable PIM-SM.

```
[CEa2] interface loopback 1
[CEa2-LoopBack1] ip address 22.22.22.22 32
[CEa2-LoopBack1] pim sm
[CEa2-LoopBack1] quit
```

Configure Loopback 1 as a C-BSR and a C-RP for VPN a.

```
[CEa2] pim
[CEa2-pim] c-bsr loopback 1
[CEa2-pim] c-rp loopback 1
[CEa2-pim] quit
```

Configure RIP

```
[CEa2] rip 2
[CEa2-rip-2] network 10.0.0.0
[CEa2-rip-2] network 22.0.0.0
```

8. Configure CE a3.

Enable IP multicast routing.

```
<CEa3> system-view
[CEa3] multicast routing-enable
```

Configure an IP address for VLAN-interface 50 and enable IGMP and PIM-SM on the interface.

```
[CEa3] interface vlan-interface 50
[CEa3-Vlan-interface50] ip address 10.110.10.1 24
[CEa3-Vlan-interface50] igmp enable
[CEa3-Vlan-interface50] pim sm
[CEa3-Vlan-interface50] quit
```

Configure an IP address for VLAN-interface 17 and enable PIM-SM on the interface.

```
[CEa3] interface vlan-interface 17
[CEa3-Vlan-interface17] ip address 10.110.5.2 24
[CEa3-Vlan-interface17] pim sm
[CEa3-Vlan-interface17] quit
```

Configure an IP address for VLAN-interface 16 and enable PIM-SM on the interface.

```
[CEa3] interface vlan-interface 16
[CEa3-Vlan-interface16] ip address 10.110.12.2 24
[CEa3-Vlan-interface16] pim sm
[CEa3-Vlan-interface16] quit
```

Configure RIP

```
[CEa3] rip 2
[CEa3-rip-2] network 10.0.0.0
```

9. Configure CE b2.

Enable IP multicast routing.

```
<CEb2> system-view
[CEb2] multicast routing-enable
```

Configure an IP address for VLAN-interface 60 and enable IGMP and PIM-SM on the interface.

```
[CEb2] interface vlan-interface 60
[CEb2-Vlan-interface60] ip address 10.110.11.1 24
[CEb2-Vlan-interface60] igmp enable
[CEb2-Vlan-interface60] pim sm
[CEb2-Vlan-interface60] quit
```

Configure an IP address for VLAN-interface 18 and enable PIM-SM on the interface.

```
[CEb2] interface vlan-interface 18
[CEb2-Vlan-interface18] ip address 10.110.6.2 24
```

```
[CEb2-Vlan-interface18] pim sm
[CEb2-Vlan-interface18] quit
```

Configure RIP

```
[CEb2] rip 3
[CEb2-rip-3] network 10.0.0.0
```

10. Verify the configuration

To view the share-group information of a VPN instance, use **display multicast-domain vpn-instance share-group**.

View the local share-group information of VPN instance a on PE 1.

```
<PE1> display multicast-domain vpn-instance a share-group local
MD local share-group information for VPN-Instance: a
  Share-group: 239.1.1.1
  MTunnel address: 1.1.1.1
```

View the local share-group information of VPN instance a on PE 2.

```
<PE2> display multicast-domain vpn-instance a share-group local
MD local share-group information for VPN-Instance: a
  Share-group: 239.1.1.1
  MTunnel address: 1.1.1.2
```

View the local share-group information of VPN instance b on PE 2.

```
<PE2> display multicast-domain vpn-instance b share-group local
MD local share-group information for VPN-Instance: b
  Share-group: 239.2.2.2
  MTunnel address: 1.1.1.2
```

View the local share-group information of VPN instance a on PE 3.

```
<PE3> display multicast-domain vpn-instance a share-group local
MD local share-group information for VPN-Instance: a
  Share-group: 239.1.1.1
  MTunnel address: 1.1.1.3
```

View the local share-group information of VPN instance b on PE 3.

```
<PE3> display multicast-domain vpn-instance b share-group local
MD local share-group information for VPN-Instance: b
  Share-group: 239.2.2.2
  MTunnel address: 1.1.1.3
```

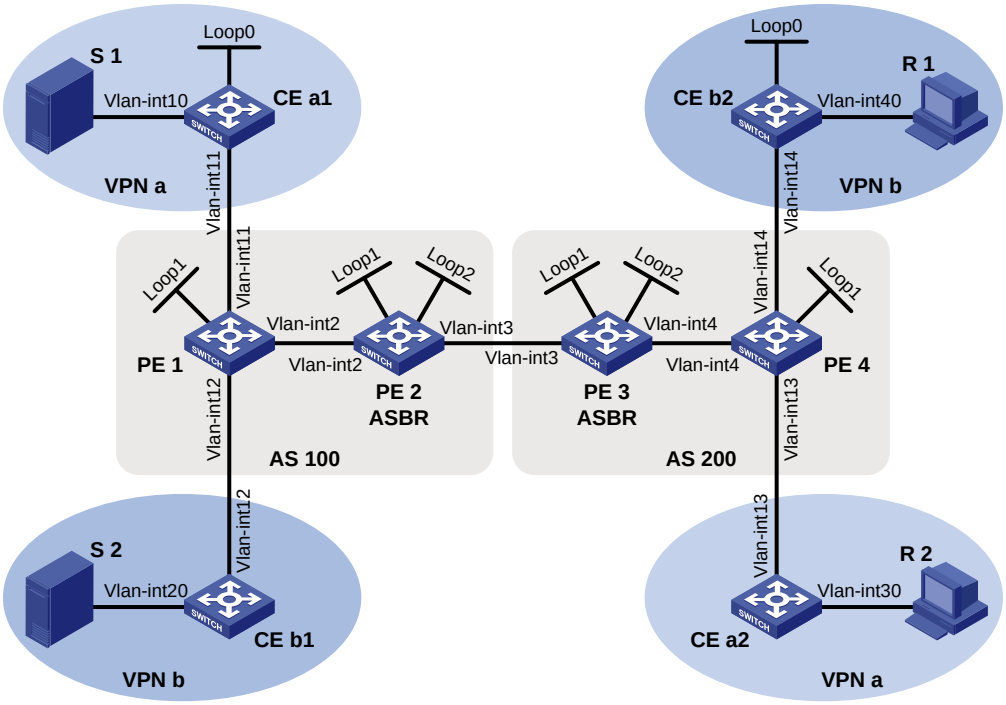
Multi-AS MD VPN configuration

Network requirements

Item	Network requirements
Multicast sources and receivers	• In VPN a, S 1 is a multicast source, and R 2 is a receiver. • In VPN b, S 2 is a multicast source, and R 1 is a receiver. • For VPN a, the share-group address is 239.1.1.1. • For VPN b, the share-group address is 239.4.4.4.

Item	Network requirements
PE interfaces and VPN instances they belong to	• PE 1—VLAN-interface 11 belongs to VPN instance b; VLAN-interface 12 belongs to VPN instance a; VLAN-interface 2 and Loopback 1 belong to the public network instance. • PE 2—VLAN-interface 2, VLAN-interface 3, Loopback 1 and Loopback 2 belong to the public network instance. • PE 3—VLAN-interface 3, VLAN-interface 4, Loopback 1 and Loopback 2 belong to the public network instance. • PE 4—VLAN-interface 13 belongs to VPN instance a; VLAN-interface 14 belongs to VPN instance b; VLAN-interface 4 and Loopback 1 belong to the public network instance.
Unicast routing protocols and MPLS	• Configure OSPF separately in AS 100 and AS 200, and configure OSPF between the PEs and CEs. • Establish BGP peer connections between PE 1, PE 2, PE 3 and PE 4 on their respective Loopback 1 interface and exchange all VPN routes between them. • Configure MPLS separately in AS 100 and AS 200.
IP multicast routing	• Enable IP multicast routing on the public network on PE 1, PE 2, PE 3 and PE 4. • Enable IP multicast routing in VPN instance a on PE 1 and PE 4. • Enable IP multicast routing in VPN instance b on PE 1 and PE 4. • Enable IP multicast routing on CE a1, CE a2, CE b1, and CE b2.
IGMP	• Run IGMPv2 on VLAN-interface 30 of CE a2. • Run IGMPv2 on VLAN-interface 40 of CE b2.
PIM	• Enable PIM-SM on all public network interfaces of PE 2 and PE 3. • Enable PIM-SM on all public and private network interfaces of PE 1 and PE 4. • Enable PIM-SM on all interfaces of CE a1, CE a2, CE b1, and CE b2. • Configure Loopback 2 of PE 2 and PE 3 as a C-BSR and a C-RP for their respective AS (to work for all multicast groups). • Configure Loopback 0 of CE a1 as a C-BSR and a C-RP for VPN a (to work for all multicast groups). • Configure Loopback 0 of CE b1 as a C-BSR and a C-RP for VPN b (to work for all multicast groups).
MSDP	• Establish an MSDP peering relationship between PE 2 and PE 3 on their respective Loopback 1.

Figure 75 Network diagram for multi-AS MD-VPN configuration



Device	Interface	IP address	Device	Interface	IP address
S 1	—	10.11.5.2/24	R 1	—	10.11.8.2/24
S 2	—	10.11.6.2/24	R 2	—	10.11.7.2/24
PE 1	Vlan-int2	10.10.1.1/24	PE 3	Vlan-int4	10.10.2.1/24
	Vlan-int11	10.11.1.1/24		Vlan-int3	192.168.1.2/24
	Vlan-int12	10.11.2.1/24		Loop1	1.1.1.3/32
	Loop1	1.1.1.1/32		Loop2	22.22.22.22/32
PE 2	Vlan-int2	10.10.1.2/24	PE 4	Vlan-int4	10.10.2.2/24
	Vlan-int3	192.168.1.1/24		Vlan-int13	10.11.3.1/24
	Loop1	1.1.1.2/32		Vlan-int14	10.11.4.1/32
	Loop2	11.11.11.11/32		Loop2	1.1.1.4/32
CE a1	Vlan-int10	10.11.5.1/24	CE b1	Vlan-int20	10.11.6.1/24
	Vlan-int11	10.11.1.2/24		Vlan-int12	10.11.2.2/24
	Loop0	2.2.2.2/32	CE b2	Vlan-int40	10.11.8.1/24
CE a2	Vlan-int30	10.11.7.1/24		Vlan-int14	10.11.4.2/24
	Vlan-int13	10.11.3.2/24		Loop0	3.3.3.3/32

Procedure

1. Configure PE 1

Configure a Router ID, enable IP multicast routing on the public network, configure an MPLS LSR ID, and enable the LDP capability.

```
<PE1> system-view
```

```
[PE1] router id 1.1.1.1
[PE1] multicast routing-enable
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
```

Create VPN instance a, configure an RD for it, and create an ingress route and an egress route for it; enable IP multicast routing in VPN instance a, configure a share-group address, and associate an MTI with the VPN instance.

```
[PE1] ip vpn-instance a
[PE1-vpn-instance-a] route-distinguisher 100:1
[PE1-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE1-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE1-vpn-instance-a] multicast routing-enable
[PE1-vpn-instance-a] multicast-domain share-group 239.1.1.1 binding mtunnel 0
[PE1-vpn-instance-a] quit
```

Create VPN instance b, configure an RD for it, and create an ingress route and an egress route for it; enable IP multicast routing in VPN instance b, configure a share-group address, and associate an MTI with the VPN instance.

```
[PE1] ip vpn-instance b
[PE1-vpn-instance-b] route-distinguisher 200:1
[PE1-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE1-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE1-vpn-instance-b] multicast routing-enable
[PE1-vpn-instance-b] multicast-domain share-group 239.4.4.4 binding mtunnel 1
[PE1-vpn-instance-b] quit
```

Configure an IP address, and enable PIM-SM and LDP capability on the public network interface VLAN-interface 2.

```
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 10.10.1.1 24
[PE1-Vlan-interface2] pim sm
[PE1-Vlan-interface2] mpls
[PE1-Vlan-interface2] mpls ldp
[PE1-Vlan-interface2] quit
```

Bind VLAN-interface 11 to VPN instance a, configure an IP address and enable PIM-SM on the interface.

```
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] ip binding vpn-instance a
[PE1-Vlan-interface11] ip address 10.11.1.1 24
[PE1-Vlan-interface11] pim sm
[PE1-Vlan-interface11] quit
```

Bind VLAN-interface 12 to VPN instance b, configure an IP address and enable PIM-SM on the interface.

```
[PE1] interface vlan-interface 12
[PE1-Vlan-interface12] ip binding vpn-instance b
[PE1-Vlan-interface12] ip address 10.11.2.1 24
```

```
[PE1-Vlan-interface12] pim sm
[PE1-Vlan-interface12] quit
```

Configure an IP address for Loopback 1, and enable PIM-SM.

```
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.1 32
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

Configure BGP.

```
[PE1] bgp 100
[PE1-bgp] group pe1-pe2 internal
[PE1-bgp] peer pe1-pe2 label-route-capability
[PE1-bgp] peer pe1-pe2 connect-interface loopback 1
[PE1-bgp] peer 1.1.1.2 group pe1-pe2
[PE1-bgp] group pe1-pe4 external
[PE1-bgp] peer pe1-pe4 as-number 200
[PE1-bgp] peer pe1-pe4 ebgp-max-hop 255
[PE1-bgp] peer 1.1.1.4 group pe1-pe4
[PE1-bgp] peer pe1-pe2 connect-interface loopback 1
[PE1-bgp] ipv4-family vpn-instance a
[PE1-bgp-a] import-route ospf 2
[PE1-bgp-a] import-route direct
[PE1-bgp-a] quit
[PE1-bgp] ipv4-family vpn-instance b
[PE1-bgp-b] import-route ospf 3
[PE1-bgp-b] import-route direct
[PE1-bgp-b] quit
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 1.1.1.4 enable
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```

With BGP peers configured on PE 1, the interfaces MTI 0 and MTI 1 will automatically obtain IP addresses, which are the loopback interface addresses specified in the BGP peer configuration. The PIM mode running on MTI 0 is the same as on the interfaces in VPN instance a, and the PIM mode running on MTI 1 is the same as on the interfaces in VPN instance b.

Configure OSPF.

```
[PE1] ospf 1
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 10.10.0.0 0.0.255.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
[PE1] ospf 2 vpn-instance a
[PE1-ospf-2] import-route bgp
[PE1-ospf-2] area 0.0.0.0
[PE1-ospf-2-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[PE1-ospf-2-area-0.0.0.0] quit
[PE1-ospf-2] quit
```

```
[PE1] ospf 3 vpn-instance b
[PE1-ospf-3] import-route bgp
[PE1-ospf-3] area 0.0.0.0
[PE1-ospf-3-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[PE1-ospf-3-area-0.0.0.0] quit
[PE1-ospf-3] quit
```

2. Configure PE 2

Configure a Router ID, enable IP multicast routing on the public network, configure an MPLS LSR ID, and enable the LDP capability.

```
<PE2> system-view
[PE2] router id 1.1.1.2
[PE2] multicast routing-enable
[PE2] mpls lsr-id 1.1.1.2
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
```

Configure an IP address, and enable PIM-SM and LDP capability on the public network interface VLAN-interface 2.

```
[PE2] interface vlan-interface 2
[PE2-Vlan-interface2] ip address 10.10.1.2 24
[PE2-Vlan-interface2] pim sm
[PE2-Vlan-interface2] mpls
[PE2-Vlan-interface2] mpls ldp
[PE2-Vlan-interface2] quit
```

Configure an IP address, and enable PIM-SM and MPLS capability on the public network interface VLAN-interface 3.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 192.168.1.1 24
[PE2-Vlan-interface3] pim sm
[PE2-Vlan-interface3] mpls
[PE2-Vlan-interface3] quit
```

Configure an IP address for Loopback 1, and enable PIM-SM.

```
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 1.1.1.2 32
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```

Configure an IP address for Loopback 2, and enable PIM-SM.

```
[PE2] interface loopback 2
[PE2-LoopBack2] ip address 11.11.11.11 32
[PE2-LoopBack2] pim sm
[PE2-LoopBack2] quit
```

Configure Loopback 2 as a C-BSR and a C-RP for the public network instance.

```
[PE2] pim
[PE2-pim] c-bsr loopback 2
[PE2-pim] c-rp loopback 2
```

```
[PE2-pim] quit
```

Configure a BSR message boundary.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] pim bsr-boundary
[PE2-Vlan-interface3] quit
```

Establish an MSDP peering relationship.

```
[PE2] msdp
[PE2-msdp] encap-data-enable
[PE2-msdp] peer 1.1.1.3 connect-interface loopback 1
```

Configure a static route.

```
[PE2] ip route-static 1.1.1.3 32 vlan-interface 3 192.168.1.2
```

Configure BGP.

```
[PE2] bgp 100
[PE2-bgp] import-route ospf 1
[PE2-bgp] group pe2-pe1 internal
[PE2-bgp] peer pe2-pe1 route-policy map2 export
[PE2-bgp] peer pe2-pe1 label-route-capability
[PE2-bgp] peer pe2-pe1 connect-interface loopback 1
[PE2-bgp] peer 1.1.1.1 group pe2-pe1
[PE2-bgp] group pe2-pe3 external
[PE2-bgp] peer pe2-pe3 as-number 200
[PE2-bgp] peer pe2-pe3 ebgp-max-hop 255
[PE2-bgp] peer pe2-pe3 route-policy map1 export
[PE2-bgp] peer pe2-pe3 label-route-capability
[PE2-bgp] peer pe2-pe3 connect-interface loopback 1
[PE2-bgp] peer 1.1.1.3 group pe2-pe3
[PE2-bgp] quit
```

Configure OSPF.

```
[PE2] ospf 1
[PE2-ospf-1] area 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 1.1.1.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 11.11.11.11 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.10.0.0 0.0.255.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Configure a route policy.

```
[PE2] route-policy map1 permit node 10
[PE2-route-policy] apply mpls-label
[PE2-route-policy] quit
[PE2] route-policy map2 permit node 10
[PE2-route-policy] if-match mpls-label
[PE2-route-policy] apply mpls-label
[PE2-route-policy] quit
```

3. Configure PE 3

Configure a Router ID, enable IP multicast routing on the public network, configure an MPLS LSR ID, and enable the LDP capability.

```
<PE3> system-view
[PE3] router id 1.1.1.3
[PE3] multicast routing-enable
[PE3] mpls lsr-id 1.1.1.3
[PE3] mpls
[PE3-mpls] quit
[PE3] mpls ldp
[PE3-mpls-ldp] quit
```

Configure an IP address, and enable PIM-SM and LDP capability on the public network interface VLAN-interface 4.

```
[PE3] interface vlan-interface 4
[PE3-Vlan-interface4] ip address 10.10.2.1 24
[PE3-Vlan-interface4] pim sm
[PE3-Vlan-interface4] mpls
[PE3-Vlan-interface4] mpls ldp
[PE3-Vlan-interface4] quit
```

Configure an IP address, and enable PIM-SM and MPLS capability on the public network interface VLAN-interface 3.

```
[PE3] interface vlan-interface 3
[PE3-Vlan-interface3] ip address 192.168.1.2 24
[PE3-Vlan-interface3] pim sm
[PE3-Vlan-interface3] mpls
[PE3-Vlan-interface3] quit
```

Configure an IP address for Loopback 1, and enable PIM-SM.

```
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 1.1.1.3 32
[PE3-LoopBack1] pim sm
[PE3-LoopBack1] quit
```

Configure an IP address for Loopback 2, and enable PIM-SM.

```
[PE3] interface loopback 2
[PE3-LoopBack2] ip address 22.22.22.22 32
[PE3-LoopBack2] pim sm
[PE3-LoopBack2] quit
```

Configure Loopback 2 as a C-BSR and a C-RP for the public network instance.

```
[PE3] pim
[PE3-pim] c-bsr loopback 2
[PE3-pim] c-rp loopback 2
[PE3-pim] quit
```

Configure a BSR message boundary.

```
[PE3] interface vlan-interface 3
[PE3-Vlan-interface3] pim bsr-boundary
[PE3-Vlan-interface3] quit
```

Establish an MSDP peering relationship.

```
[PE3] msdp
```

```
[PE3-msdp] encap-data-enable
[PE3-msdp] peer 1.1.1.2 connect-interface loopback 1
```

Configure a static route.

```
[PE3] ip route-static 1.1.1.2 32 vlan-interface 3 192.168.1.1
```

Configure BGP.

```
[PE3] bgp 200
[PE3-bgp] import-route ospf 1
[PE3-bgp] group pe3-pe4 internal
[PE3-bgp] peer pe3-pe4 route-policy map2 export
[PE3-bgp] peer pe3-pe4 label-route-capability
[PE3-bgp] peer pe3-pe4 connect-interface loopback 1
[PE3-bgp] peer 1.1.1.4 group pe3-pe4
[PE3-bgp] group pe3-pe2 external
[PE3-bgp] peer pe3-pe2 as-number 100
[PE3-bgp] peer pe3-pe2 ebgp-max-hop 255
[PE3-bgp] peer pe3-pe2 route-policy map1 export
[PE3-bgp] peer pe3-pe2 label-route-capability
[PE3-bgp] peer pe3-pe2 connect-interface loopback 1
[PE3-bgp] peer 1.1.1.2 group pe3-pe2
[PE3-bgp] quit
```

Configure OSPF.

```
[PE3] ospf 1
[PE3-ospf-1] area 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 1.1.1.3 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 22.22.22.22 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 10.10.0.0 0.0.255.255
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

Configure a route policy.

```
[PE3] route-policy map1 permit node 10
[PE3-route-policy] apply mpls-label
[PE3-route-policy] quit
[PE3] route-policy map2 permit node 10
[PE3-route-policy] if-match mpls-label
[PE3-route-policy] apply mpls-label
[PE3-route-policy] quit
```

4. Configure PE 4

Configure a Router ID, enable IP multicast routing on the public network, configure an MPLS LSR ID, and enable the LDP capability.

```
<PE4> system-view
[PE4] router id 1.1.1.4
[PE4] multicast routing-enable
[PE4] mpls lsr-id 1.1.1.4
[PE4] mpls
[PE4-mpls] quit
[PE4] mpls ldp
```

```
[PE4-mpls-ldp] quit
```

Create VPN instance a, configure an RD for it, and create an ingress route and an egress route for it; enable IP multicast routing in VPN instance a, configure a share-group address, and associate an MTI with the VPN instance.

```
[PE4] ip vpn-instance a
[PE4-vpn-instance-a] route-distinguisher 100:1
[PE4-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE4-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE4-vpn-instance-a] multicast routing-enable
[PE4-vpn-instance-a] multicast-domain share-group 239.1.1.1 binding mtunnel 0
[PE4-vpn-instance-a] quit
```

Create VPN instance b, configure an RD for it, and create an ingress route and an egress route for it; enable IP multicast routing in VPN instance b, configure a share-group address, and associate an MTI with the VPN instance.

```
[PE4] ip vpn-instance b
[PE4-vpn-instance-b] route-distinguisher 200:1
[PE4-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE4-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE4-vpn-instance-b] multicast routing-enable
[PE4-vpn-instance-b] multicast-domain share-group 239.4.4.4 binding mtunnel 1
[PE4-vpn-instance-b] quit
```

Configure an IP address, and enable PIM-SM and LDP capability on the public network interface VLAN-interface 4.

```
[PE4] interface vlan-interface 4
[PE4-Vlan-interface4] ip address 10.10.2.2 24
[PE4-Vlan-interface4] pim sm
[PE4-Vlan-interface4] mpls
[PE4-Vlan-interface4] mpls ldp
[PE4-Vlan-interface4] quit
```

Bind VLAN-interface 13 to VPN instance a, configure an IP address and enable PIM-SM on the interface.

```
[PE4] interface vlan-interface 13
[PE4-Vlan-interface13] ip binding vpn-instance a
[PE4-Vlan-interface13] ip address 10.11.3.1 24
[PE4-Vlan-interface13] pim sm
[PE4-Vlan-interface13] quit
```

Bind VLAN-interface 14 to VPN instance b, configure an IP address and enable PIM-SM on the interface.

```
[PE4] interface vlan-interface 14
[PE4-Vlan-interface14] ip binding vpn-instance b
[PE4-Vlan-interface14] ip address 10.11.4.1 24
[PE4-Vlan-interface14] pim sm
[PE4-Vlan-interface14] quit
```

Configure an IP address for Loopback 1, and enable PIM-SM.

```
[PE4] interface loopback 1
[PE4-LoopBack1] ip address 1.1.1.4 32
```

```
[PE4-LoopBack1] pim sm
[PE4-LoopBack1] quit
```

Configure BGP.

```
[PE4] bgp 200
[PE4-bgp] group pe4-pe3 internal
[PE4-bgp] peer pe4-pe3 label-route-capability
[PE4-bgp] peer pe4-pe3 connect-interface loopback 1
[PE4-bgp] peer 1.1.1.3 group pe4-pe3
[PE4-bgp] group pe4-pe1 external
[PE4-bgp] peer pe4-pe1 as-number 100
[PE4-bgp] peer pe4-pe1 ebgp-max-hop 255
[PE4-bgp] peer 1.1.1.1 group pe4-pe1
[PE4-bgp] peer pe4-pe1 connect-interface loopback 1
[PE4-bgp] ipv4-family vpn-instance a
[PE4-bgp-a] import-route ospf 2
[PE4-bgp-a] import-route direct
[PE4-bgp-a] quit
[PE4-bgp] ipv4-family vpn-instance b
[PE4-bgp-b] import-route ospf 3
[PE4-bgp-b] import-route direct
[PE4-bgp-b] quit
[PE4-bgp] ipv4-family vpnv4
[PE4-bgp-af-vpnv4] peer 1.1.1.1 enable
[PE4-bgp-af-vpnv4] quit
[PE4-bgp] quit
```

With BGP peers configured on PE 4, the interfaces MTI 0 and MTI 1 will automatically obtain IP addresses, which are the loopback interface addresses specified in the BGP peer configuration. The PIM mode running on MTI 0 is the same as on the interfaces in VPN instance a, and the PIM mode running on MTI 1 is the same as on the interfaces in VPN instance b.

Configure OSPF.

```
[PE4] ospf 1
[PE4-ospf-1] area 0.0.0.0
[PE4-ospf-1-area-0.0.0.0] network 1.1.1.4 0.0.0.0
[PE4-ospf-1-area-0.0.0.0] network 10.10.0.0 0.0.255.255
[PE4-ospf-1-area-0.0.0.0] quit
[PE4-ospf-1] quit
[PE4] ospf 2 vpn-instance a
[PE4-ospf-2] import-route bgp
[PE4-ospf-2] area 0.0.0.0
[PE4-ospf-2-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[PE4-ospf-2-area-0.0.0.0] quit
[PE4-ospf-2] quit
[PE4] ospf 3 vpn-instance b
[PE4-ospf-3] import-route bgp
[PE4-ospf-3] area 0.0.0.0
[PE4-ospf-3-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[PE4-ospf-3-area-0.0.0.0] quit
```

```
[PE4-ospf-3] quit
```

5. Configure CE a1

Enable IP multicast routing.

```
<CEa1> system-view
[CEa1] multicast routing-enable
```

Configure an IP address for VLAN-interface 10 and enable PIM-SM on the interface.

```
[CEa1] interface vlan-interface 10
[CEa1-Vlan-interface10] ip address 10.11.5.1 24
[CEa1-Vlan-interface10] pim sm
[CEa1-Vlan-interface10] quit
```

Configure an IP address for VLAN-interface 11 and enable PIM-SM on the interface.

```
[CEa1] interface vlan-interface 11
[CEa1-Vlan-interface11] ip address 10.11.1.2 24
[CEa1-Vlan-interface11] pim sm
[CEa1-Vlan-interface11] quit
```

Configure an IP address for Loopback 1, and enable PIM-SM.

```
[CEa1] interface loopback 1
[CEa1-LoopBack1] ip address 2.2.2.2 32
[CEa1-LoopBack1] pim sm
[CEa1-LoopBack1] quit
```

Configure Loopback 1 as a C-BSR and a C-RP for VPN a.

```
[CEa1] pim
[CEa1-pim] c-bsr loopback 1
[CEa1-pim] c-rp loopback 1
[CEa1-pim] quit
```

Configure OSPF.

```
[CEa1] ospf 1
[CEa1-ospf-1] area 0.0.0.0
[CEa1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[CEa1-ospf-1-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[CEa1-ospf-1-area-0.0.0.0] quit
[CEa1-ospf-1] quit
```

6. Configure CE b1

Enable IP multicast routing.

```
<CEb1> system-view
[CEb1] multicast routing-enable
```

Configure an IP address for VLAN-interface 20 and enable PIM-SM on the interface.

```
[CEb1] interface vlan-interface 20
[CEb1-Vlan-interface20] ip address 10.11.6.1 24
[CEb1-Vlan-interface20] pim sm
[CEb1-Vlan-interface20] quit
```

Configure an IP address for VLAN-interface 12 and enable PIM-SM on the interface.

```
[CEb1] interface vlan-interface 12
[CEb1-Vlan-interface12] ip address 10.11.2.2 24
```

```
[CEb1-Vlan-interface12] pim sm
[CEb1-Vlan-interface12] quit
```

Configure OSPF.

```
[CEb1] ospf 1
[CEb1-ospf-1] area 0.0.0.0
[CEb1-ospf-1-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[CEb1-ospf-1-area-0.0.0.0] quit
[CEb1-ospf-1] quit
```

7. Configure CE a2

Enable IP multicast routing.

```
<CEa2> system-view
[CEa2] multicast routing-enable
```

Configure an IP address for VLAN-interface 30 and enable IGMP and PIM-SM on the interface.

```
[CEa2] interface vlan-interface 30
[CEa2-Vlan-interface30] ip address 10.11.7.1 24
[CEa2-Vlan-interface30] igmp enable
[CEa2-Vlan-interface30] pim sm
[CEa2-Vlan-interface30] quit
```

Configure an IP address for VLAN-interface 13 and enable PIM-SM on the interface.

```
[CEa2] interface vlan-interface 13
[CEa2-Vlan-interface13] ip address 10.11.3.2 24
[CEa2-Vlan-interface13] pim sm
[CEa2-Vlan-interface13] quit
```

Configure OSPF.

```
[CEa2] ospf 1
[CEa2-ospf-1] area 0.0.0.0
[CEa2-ospf-1-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[CEa2-ospf-1-area-0.0.0.0] quit
[CEa2-ospf-1] quit
```

8. Configure CE b2

Enable IP multicast routing.

```
<CEb2> system-view
[CEb2] multicast routing-enable
```

Configure an IP address for VLAN-interface 40 and enable IGMP and PIM-SM on the interface.

```
[CEb2] interface vlan-interface 40
[CEb2-Vlan-interface40] ip address 10.11.8.1 24
[CEb2-Vlan-interface40] igmp enable
[CEb2-Vlan-interface40] pim sm
[CEb2-Vlan-interface40] quit
```

Configure an IP address for VLAN-interface 14 and enable PIM-SM on the interface.

```
[CEb2] interface vlan-interface 14
[CEb2-Vlan-interface14] ip address 10.11.4.2 24
[CEb2-Vlan-interface14] pim sm
[CEb2-Vlan-interface14] quit
```

Configure an IP address for Loopback 1, and enable PIM-SM.

```
[CEb2] interface loopback 1
[CEb2-LoopBack1] ip address 3.3.3.3 32
[CEb2-LoopBack1] pim sm
[CEb2-LoopBack1] quit
```

Configure Loopback 1 as a C-BSR and a C-RP for VPN b.

```
[CEb2] pim
[CEb2-pim] c-bsr loopback 1
[CEb2-pim] c-rp loopback 1
[CEb2-pim] quit
```

Configure OSPF.

```
[CEb2] ospf 1
[CEb2-ospf-1] area 0.0.0.0
[CEb2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[CEb2-ospf-1-area-0.0.0.0] network 10.11.0.0 0.0.255.255
[CEb2-ospf-1-area-0.0.0.0] quit
[CEb2-ospf-1] quit
```

9. Verify the configuration

To view the share-group information of a VPN instance, use **display multicast-domain vpn-instance share-group**.

View the local share-group information of VPN instance a on PE 1.

```
<PE1> display multicast-domain vpn-instance a share-group local
MD local share-group information for VPN-Instance: a
  Share-group: 239.1.1.1
  MTunnel address: 1.1.1.1
```

View the local share-group information of VPN instance b on PE 1.

```
<PE1> display multicast-domain vpn-instance b share-group local
MD local share-group information for VPN-Instance: b
  Share-group: 239.4.4.4
  MTunnel address: 1.1.1.1
```

View the local share-group information of VPN instance a on PE 4.

```
<PE4> display multicast-domain vpn-instance a share-group local
MD local share-group information for VPN-Instance: a
  Share-group: 239.1.1.1
  MTunnel address: 1.1.1.4
```

View the local share-group information of VPN instance b on PE 4.

```
<PE4> display multicast-domain vpn-instance b share-group local
MD local share-group information for VPN-Instance: b
  Share-group: 239.4.4.4
  MTunnel address: 1.1.1.4
```

Troubleshooting MD-VPN configuration

Unable to establish a share-MDT

Symptom

A share-MDT cannot be established. PIM adjacencies cannot be established between the same VPN instance's interfaces on different PE devices.

Analysis

- On different PE devices, the same share-group must be configured for the same VPN instance. A share-group address uniquely identifies a share-MDT. If different share-group addresses have been configured for a VPN instance on different PE devices, a share-MDT cannot be established for that VPN instance on different PE devices.
- The same PIM mode must run on all the interfaces of the same VPN instance on different PE devices and on all the interfaces of the P router. Otherwise, a share-MDT cannot be correctly built for the VPN instance and PIM adjacencies cannot be established between the VPN instance on the local PE device and the same VPN instance on the remote PE device.
- BGP and unicast route configurations are prerequisites for the MTI interface to obtain an IP address automatically, and PIM is enabled on at least one interface of the VPN instance so that PIM can be enabled on the MTI interface. PIM adjacencies can be established between the same VPN instance on different PE devices only after the MTI interface obtains an IP address and gets PIM enabled.

Solution

1. Check the share-group address. Use **display multicast-domain vpn-instance share-group** to verify that the same share-group address has been configured for the same VPN instance on different PE devices.
2. Check the running PIM mode. Use **display pim interface** to verify that PIM is enabled on at least one interface of the same VPN on different PE devices and the same PIM mode is running on all the interfaces of the same VPN instance on different PE devices and on all the interfaces of the P router.
3. Check unicast routes. Use **display ip routing-table** to verify that a unicast route exists from the VPN instance on the local PE device to the same VPN instance on each remote PE device.
4. Check BGP peer configuration. Use **display bgp peer** to verify that the BGP peer connections have been correctly configured.

Unable to build an MVRF

Symptom

A VPN instance cannot create an MVRF correctly.

Analysis

- If PIM-SM is running in the VPN instance, the BSR information for the VPN instance is required. Otherwise, the VPN instance's MVRF cannot be correctly established.
- If PIM-SM is running in the VPN instance, the RP information for the VPN instance is required. If a unicast route to the RP is not available, this means that a PIM adjacency has not been correctly established between the public network and the VPN instance, and thus VPN instance cannot correctly establish its MVRF.

- The customer DR must have a route to the VPN RP.

Solution

1. Use **display pim bsr-info** to check whether the BSR information exists on the public network and VPN instance. If not, check whether a unicast route exists to the BSR.
2. Use **display pim rp-info** to view the RP information. If no RP information is available, check whether a unicast route exists to the RP. Use **display pim neighbor** to check whether the PIM adjacencies have correctly established in the public network and the VPN.
3. Use **ping** to check the connectivity between the VPN DR and the VPN RP.

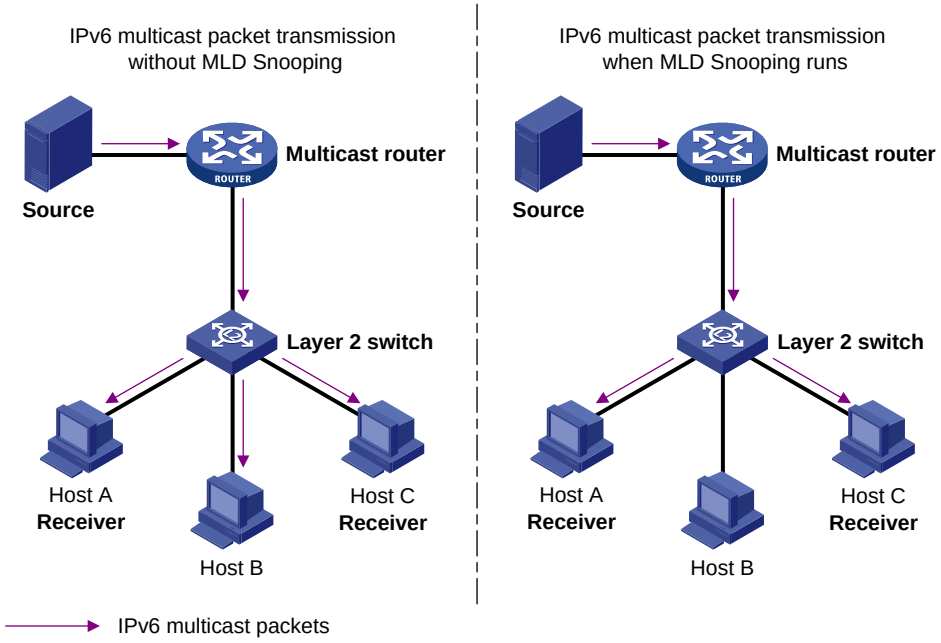
Configuring MLD snooping

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 switch that is running MLD snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.

As shown in Figure 76, when MLD snooping is not running, IPv6 multicast packets are broadcast to all devices at Layer 2. When MLD snooping runs, multicast packets for known IPv6 multicast groups are multicast to the receivers at Layer 2.

Figure 76 Before and after MLD snooping is enabled on the Layer 2 device



MLD snooping forwards multicast data to the receivers that require it at Layer 2 only and provides the following advantages:

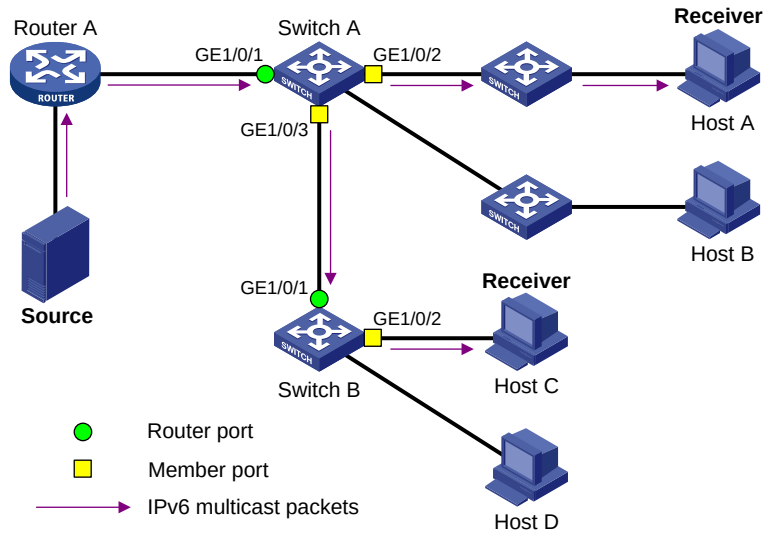
- Reducing Layer 2 broadcast packets, thus saving network bandwidth.
- Enhancing the security of multicast traffic.
- Facilitating the implementation of per-host accounting.

Basic concepts in MLD snooping

MLD snooping related ports

As shown in Figure 77, 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 (IPv6 multicast group members).

Figure 77 MLD snooping related ports



Ports involved in MLD snooping, as shown in Figure 77, are described as follows:

- Router port—A router port is a port on the Ethernet switch that leads the switch toward the Layer-3 multicast device (DR or 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 local router ports in its router port list.
- Member port—A member port (also known as "IPv6 multicast group member port") is a port on the Ethernet switch that leads toward multicast group members. 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 the member ports on the local switch in its MLD snooping forwarding table.

Whenever mentioned in this document, a router port is a router-connecting port on the switch, rather than a port on a router.

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

On an MLD snooping-enabled switch, the ports that received MLD general queries with the source address other than 0::0 or IPv6 PIM hello messages are dynamic router ports. For more information about IPv6 PIM hello messages, see *IP Multicast Configuration Guide*.

Aging timers for dynamic ports in MLD snooping

Table 11 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 sets a timer initialized to the dynamic router port aging time.	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.
Dynamic member port aging timer	When a port dynamically joins an IPv6 multicast group, the switch sets a timer for the port, which is initialized to the dynamic member port aging time.	MLD report message.	The switch removes this port from the MLD snooping forwarding table.

The port aging mechanism of MLD snooping works only for dynamic ports; a static port will never age out.

How MLD snooping works

A switch that is running MLD snooping performs different actions when it receives different MLD messages.

The description about adding or deleting a port in this section is only for a dynamic port. Static ports can be added or deleted only through the corresponding configurations.

General queries

The MLD querier periodically sends MLD general queries to all hosts and routers (FF02::1) on the local subnet to determine whether IPv6 multicast group members exist on the subnet.

After receiving an MLD general query, the switch forwards it through all ports in the VLAN except the port that received the MLD query. The switch evaluates the following:

- If the port that received the MLD query is a dynamic router port in its router port list, the switch resets the aging timer for this dynamic router port.
- If the port is not included in its router port list, the switch adds it into its router port list as a dynamic router port and sets an aging timer for it.

Membership reports

A host sends an MLD report to the MLD querier in the following circumstances:

- Upon receiving an MLD query, an IPv6 multicast group member host responds with an MLD report.
- When intended to join an IPv6 multicast group, a host sends an MLD report to the MLD querier to announce that it is available for the multicast information addressed to that IPv6 multicast group.

Upon 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 the following to the receiving port:

- If no forwarding table entry exists for the reported IPv6 multicast group, the switch creates an entry, adds the port as a dynamic member port to the outgoing port list, and starts a member port aging timer for that port.
- If a forwarding table entry exists for the reported IPv6 multicast group, but the port is not included in the outgoing port list for that group, the switch adds the port as a dynamic member port to the outgoing port list, and starts a member port aging timer for that port.
- If a forwarding table entry exists for the reported IPv6 multicast group and the port is included in the outgoing port list, which means that this port is already a dynamic member port, the switch resets the member port aging timer for that port.

A switch does not forward an MLD report through a non-router port. This is because if the switch forwards a report message through a member port, all the attached hosts listening to the reported IPv6 multicast address will suppress their own reports upon receiving this report according to the MLD report suppression mechanism for hosts, and this will prevent the switch from knowing 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 *IP Multicast Configuration Guide*.

Done messages

When a host leaves an IPv6 multicast group, the host sends an MLD done message to the multicast router.

When the switch receives an MLD done message on a dynamic member port, the switch first determines whether a forwarding table entry for the IPv6 multicast group address in the message exists, and, if one exists, whether the outgoing port list contains the port.

- If the forwarding table entry does not exist or if the outgoing port list does not contain the port, the switch discards the MLD done message instead of forwarding it to any port.
- If the forwarding table entry exists and the outgoing port list contains the port, the switch forwards the MLD done message to all router ports in the native VLAN. Because the switch has not determined whether any other hosts attached to the port are still monitoring that IPv6 multicast group address, the switch does not immediately remove the port from the outgoing port list of the forwarding table entry for that group. Instead, it resets the aging timer for the port.

After receiving an MLD done message from a host, 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 address through the port that received the MLD done message. After receiving the MLD multicast-address-specific query, the switch forwards it through all the router ports in the VLAN and all member ports for that IPv6 multicast group, and performs the following to the receiving port:

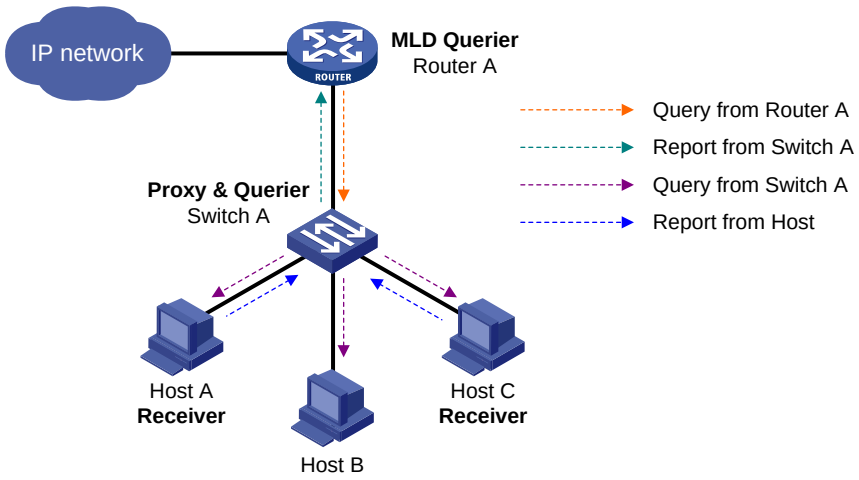
- If the port receives any MLD report in response to the MLD multicast-address-specific query (suppose it is a dynamic member port) before its aging timer expires, this means that a host attached to the port is receiving or expecting to receive IPv6 multicast data for that IPv6 multicast group. The switch resets the aging timer for the port.
- If no MLD report in response to the MLD multicast-address-specific query is received on the port before its aging timer expires, this means that no hosts attached to the port are still monitoring that IPv6 multicast group address. The switch removes the port from the outgoing port list of the forwarding table entry for that 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.

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 *IP Multicast Configuration Guide*.

Figure 78 Figure Network diagram for MLD snooping proxying



As shown in Figure 78, 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 12 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 it maintains and sends the report out 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 all router ports if the forwarding entry for the group still contains a member port.
Report	When receiving a report for an IPv6 multicast group, the proxy looks up the multicast forwarding table for the entry for the multicast group. If the forwarding entry is found with the receiving port contained as a dynamic port in the outgoing port list, the proxy resets the aging timer for the entry. If the forwarding entry is found but the outgoing port list does not include the receiving port, the proxy adds the port to the outgoing port list as a dynamic member port and starts an aging timer for it. If no forwarding entry is found, the proxy creates the entry, adds the receiving port to the outgoing port list as a dynamic member port and starts an aging timer for the port, and then, sends a report to the group out all router ports.
Done	In response to a done message for an IPv6 multicast group, the proxy sends a multicast-address-specific query for the group out 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 all router ports.

Processing of IPv6 multicast protocol messages

With Layer 3 multicast routing enabled, an MLD snooping switch processes IPv6 multicast protocol messages differently under different conditions, specifically as follows:

- If only MLD is enabled on the switch, or if both MLD and IPv6 PIM are enabled on the switch, the switch handles IPv6 multicast protocol messages in the normal way.
- If only IPv6 PIM is enabled on the switch, the following occur:
  - The switch broadcasts MLD messages as unknown messages in the VLAN.
  - Upon receiving an IPv6 PIM hello message, the switch maintains the corresponding dynamic router port.
- When 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 without deleting its dynamic router ports.

Protocols and standards

MLD snooping is documented in RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches.

MLD snooping configuration tasks

Configurations made in MLD snooping view are effective for all VLANs, while configurations made in VLAN view are effective only for ports belonging to the current VLAN. For a given VLAN, a configuration made in MLD snooping view is effective only if the same configuration is not made in VLAN view.

Configurations made in MLD snooping view are effective for all ports; configurations made in Ethernet interface view are effective only for the current port; configurations made in Layer 2 aggregate interface view are effect only for the current interface; configurations made in port group view are effective only for all the ports in the current port group. For a given port, a configuration made in MLD snooping view is effective only if the same configuration is not made in Ethernet interface view, Layer 2 aggregate interface view or port group view.

For MLD snooping, configurations made on a Layer 2 aggregate interface do not interfere with configurations made on its member ports, nor do they take part in aggregation calculations; configurations made on a member port of the aggregate group will not take effect until it leaves the aggregate group.

Configuring basic functions of MLD snooping

Prerequisites

Before configuring the basic functions of MLD snooping, complete the following tasks:

- Configure the corresponding VLANs
- Determine the version of MLD snooping

Enabling MLD snooping

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enable MLD snooping globally and enter MLD snooping view.	**mld-snooping**	Required. Defaults to disabled.
3. Return to system view.	**quit**	—
4. Enter VLAN view.	**vlan** *vlan-id*	—
5. Enable MLD snooping in the VLAN.	**mld-snooping enable**	Required. Defaults to disabled.

MLD snooping must be enabled globally before it can be enabled in a VLAN.

After enabling MLD snooping in a VLAN, you cannot enable MLD and/or IPv6 PIM on the corresponding VLAN interface, and vice versa.

When you enable MLD snooping in a specified VLAN, this function takes effect for ports in this VLAN only.

Configuring the version of MLD snooping

By configuring the MLD snooping version, you actually configure the version of MLD messages that MLD snooping can process.

- MLD snooping version 1 can process MLDv1 messages, but cannot analyze and process MLDv2 messages, which will be flooded in the VLAN.
- MLD snooping version 2 can process MLDv1 and MLDv2 messages.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Configure the version of MLD snooping.	**mld-snooping version** *version-number*	Optional. Version 1 by default.

If you switch MLD snooping from version 2 to version 1, the system will clear all MLD snooping forwarding entries from dynamic joining, and will:

- Keep forwarding entries from version 2 static (*, G) joining.
- Clear forwarding entries from version 2 static (S, G) joining, which are restored when MLD snooping is switched back to version 2.

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. You can also configure IPv6 multicast MAC address entries.

Configuring an IPv6 static multicast MAC address entry in system view

Table 13 Configure an IPv6 static multicast MAC address entry in system view

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Configure a static multicast MAC address entry.	**mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	Required. No static multicast MAC address entries exist by default.

Configuring an IPv6 static multicast MAC address entry in interface view

Table 14 Configure an IPv6 static multicast MAC address entry in interface view

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number*	Required. In Ethernet interface view or Layer 2 aggregate interface view, the configuration takes effect on only the current interface. In port group view, the configuration takes effect on all ports in the port group.

To do...	Use the command...	Remarks
3. Configure a static multicast MAC address entry.	**mac-address multicast** *mac-address* **vlan** *vlan-id*	Required. No static multicast MAC address entries exist by default.

For more information about the **mac-address multicast** command, see *IP Multicast Command Reference*.

When configuring a static multicast MAC address entry in system view, the configuration is effective for the specified interface. When configuring a static multicast MAC address entry in interface view or port group view, the configuration is effective only for the current interface or interfaces in the current port group.

Any legal IPv6 multicast MAC address except 3333-xxxx-xxxx (with x representing a hexadecimal number from 0 to F) can be manually added to the MAC address table.

Configuring MLD snooping port functions

Prerequisites

Before configuring 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 timer of dynamic member ports
- Determine the IPv6 multicast group and IPv6 multicast source addresses

Configuring aging timers for dynamic ports

If the switch receives no MLD general queries or IPv6 PIM hello messages on a dynamic router port, the switch removes the port from the router port list when the aging timer of the port expires.

If the switch receives no MLD reports for an IPv6 multicast group on a dynamic member port, the switch removes the port from the outgoing port list of the forwarding table entry for that IPv6 multicast group when the port aging timer expires.

If IPv6 multicast group memberships change frequently, set a relatively small value for the dynamic member port aging timer.

Configuring aging timers for dynamic ports globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter MLD snooping view.	**mld-snooping**	—
3. Configure dynamic router port aging time.	**router-aging-time** *interval*	Optional. Defaults to 260 seconds.

To do...	Use the command...	Remarks
4. Configure dynamic member port aging time.	**host-aging-time** *interval*	Optional. Defaults to 260 seconds.

Configuring aging timers for dynamic ports in a VLAN

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Configure dynamic router port aging time.	**mld-snooping router-aging-time** *interval*	Optional. Defaults to 260 seconds.
4. Configure dynamic member port aging time.	**mld-snooping host-aging-time** *interval*	Optional. Defaults to 260 seconds.

Configuring static ports

If all the hosts attached to a port are available for the IPv6 multicast data addressed to a particular IPv6 multicast group, configure that port as a static member port for that IPv6 multicast group.

You can configure a port of a switch to be a static router port, through which the switch can forward all IPv6 multicast data it received.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Configure the port(s) as static member port(s).	**mld-snooping static-group** *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*	Required. No static member ports by default.
4. Configure the port(s) as static router port(s).	**mld-snooping static-router-port** vlan *vlan-id*	Required. No static router ports by default.

An IPv6 static (S, G) join takes effect only if a valid IPv6 multicast source address is specified and MLD snooping version 2 is currently running.

A static member port does not respond to queries from the MLD querier. When static (*, G) or (S, G) joining is enabled or disabled on a port, the port does not send an unsolicited MLD report or an MLD done message.

If MLD is enabled on the virtual interface of a VLAN on a switch and you want a port in that VLAN to be a static member port for an IPv6 multicast group or an IPv6 multicast source and group, in addition to configuring the port as a static member port, you must use **mld static-group** to configure the VLAN interface to be a static member of the IPv6 multicast group or source and group. For more information about **mld static-group**, see *IP Multicast Command Reference*.

Static member ports and static router ports never age out. To remove such a port, you must use the corresponding **undo** command.

Configuring simulated joining

Generally, a host that is running MLD responds to MLD queries from the MLD querier. If a host fails to respond, the multicast router will deem that no member of this IPv6 multicast group exists on the network segment, and will remove the corresponding forwarding path.

To avoid this situation, enable simulated joining on a port of the switch. Namely, you can configure the port as a simulated member host for an IPv6 multicast group. When an MLD query is received, the simulated host gives a response. Thus, the switch can continue receiving IPv6 multicast data.

A simulated host acts like a real host, as follows:

- When a port is configured as a simulated member host, the switch sends an unsolicited MLD report through that port.
- After a port is configured as a simulated member host, the switch responds to MLD general queries by sending MLD reports through that port.
- When the simulated joining function is disabled on a port, the switch sends an MLD done message through that port.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Configure simulated joining.	**mld-snooping host-join** *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*	Required. Defaults to disabled.

Each simulated host is equivalent to an independent host. For example, when receiving an MLD query, the simulated host corresponding to each configuration responds respectively.

Unlike a static member port, a port configured as a simulated member host will age out like a dynamic member port.

Configuring fast leave processing

The fast leave processing feature enables the switch to process MLD done messages quickly. When the fast leave processing feature is enabled and the switch receives an MLD done message on a port, the switch immediately removes that port from the outgoing port list of the forwarding table entry for the indicated IPv6 multicast group. Then, when receiving MLD done multicast-address-specific queries for that IPv6 multicast group, the switch will not forward them to that port.

In VLANs where only one host is attached to each port, fast leave processing helps improve bandwidth and resource usage. However, if fast leave processing is enabled on a port to which more than one host is attached, when one host leaves a multicast group, the other hosts attached to the port and available for the same multicast group will fail to receive multicast data for that group. Therefore, if the function of

dropping unknown IPv6 multicast traffic is already enabled on the switch or in the VLANs, you should not enable the fast leave processing function.

Configuring fast leave processing globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter MLD snooping view.	**mld-snooping**	—
3. Enable fast leave processing.	**fast-leave** [**vlan** *vlan-list*]	Required. Defaults to disabled.

Configuring fast leave processing on a port or a group of ports

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Enable fast leave processing.	**mld-snooping fast-leave** [**vlan** *vlan-list*]	Required. Defaults to disabled.

Disabling a port or a group of ports from changing into dynamic router ports

At present, 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 switch port becomes a dynamic router port. Before its timer expires, this dynamic router port will receive all multicast packets within the VLAN it belongs to and forward then to the host, thus affecting normal multicast reception of the host.
- In addition, the MLD general query and IPv6 PIM Hello message sent from the host 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 switch port from changing into a dynamic router port upon receiving an MLD general query or IPv6 PIM Hello message; thus, network security and control over multicast users are enhanced.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.

To do...	Use the command...	Remarks
3. Disable the port or group of ports from changing into dynamic router ports.	**mld-snooping router-port-deny** [**vlan** *vlan-list*]	Required. By default, the port or group of ports can change into dynamic router ports.

This configuration does not affect the static router port configuration.

Configuring MLD snooping querier

Prerequisites

Before configuring 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 is running MLD, a multicast router or Layer 3 multicast switch sends periodic MLD general 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."

However, a Layer 2 multicast switch does not support MLD, and therefore cannot send MLD general queries by default. By enabling MLD snooping querier on a Layer 2 switch in a VLAN where multicast traffic must be Layer-2 switched only and no Layer 3 multicast devices are present, the Layer 2 switch will act as the MLD querier to send periodic MLD queries. Multicast forwarding entries can then be established and maintained at the data link layer.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Enable the MLD snooping querier.	**mld-snooping querier**	Required. Defaults to disabled.

It is meaningless to configure an MLD snooping querier in an IPv6 multicast network that is running 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.

For more information about the MLD querier, see *IP Multicast Configuration Guide*.

Configuring MLD queries and responses

You can tune the MLD general query interval based on the actual condition of the network.

Upon receiving an MLD query (general query or multicast-address-specific query), a host starts a timer for each IPv6 multicast group that it has joined. This timer is initialized to a random value in the range of 0 to the maximum response time. (the host obtains the value of the maximum response time from the Max Response Time field in the MLD query that it received.) When the timer value comes down to 0, the host sends an MLD report to the corresponding IPv6 multicast group.

An appropriate setting of the maximum response time for MLD queries enables hosts to respond to queries quickly and avoids bursts of MLD traffic on the network. Such bursts can occur when a large number of hosts simultaneously send reports when the corresponding timers expire simultaneously.

- For MLD general queries, configure the maximum response time to fill their Max Response time field.
- For MLD multicast-address-specific queries, configure the MLD last-member query interval to fill their Max Response time field. Namely, for MLD multicast-address-specific queries, the maximum response time equals the MLD last-member query interval.

Configuring MLD queries and responses globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter MLD snooping view.	**mld-snooping**	—
3. Configure the maximum response time for MLD general queries.	**max-response-time** *interval*	Optional. 10 seconds by default
4. Configure the MLD last-member query interval.	**last-listener-query-interval** *interval*	Optional. 1 second by default

Configuring MLD queries and responses in a VLAN

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Configure MLD query interval.	**mld-snooping query-interval** *interval*	Optional. 125 seconds by default.
4. Configure the maximum response time for MLD general queries.	**mld-snooping max-response-time** *interval*	Optional. 10 seconds by default.
5. Configure the MLD last-member query interval.	**mld-snooping last-listener-query-interval** *interval*	Optional. 1 second by default.

Make sure that the MLD query interval is greater than the maximum response time for MLD general queries; otherwise undesired deletion of IPv6 multicast members can occur.

Configuring source IPv6 addresses of MLD queries

This configuration allows you to change the source IPv6 address of MLD queries.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Configure the source IPv6 address of MLD general queries.	**mld-snooping general-query source-ip** { *ipv6-address* | **current-interface** }	Optional. 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** { *ipv6-address* | **current-interface** }	Optional FE80::02FF:FFFF:FE00:0001 by default.

The source IPv6 address of MLD query messages may affect MLD querier election within the segment.

Configuring MLD snooping proxying

Prerequisites

- Before configuring MLD snooping proxying in a VLAN, enable MLD snooping in the VLAN and prepare the following data:
- 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Enable MLD snooping proxying in the VLAN.	**mld-snooping proxying enable**	Required. Defaults to disabled.

Configuring a source IPv6 address for the MLD messages sent by the proxy

You can set the source IPv6 addresses in the MLD reports and done messages sent by the MLD snooping proxy on behalf of its attached hosts.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—

To do...	Use the command...	Remarks
3. Configure a source IPv6 address for the MLD reports sent by the proxy.	**mld-snooping report source-ip** { *ipv6-address* | **current-interface** }	Required. The default is FE80::02FF:FFFF:FE00:0001.
4. Configure a source IPv6 address for the MLD done messages sent by the proxy.	**mld-snooping done source-ip** { *ipv6-address* | **current-interface** }	The default is FE80::02FF:FFFF:FE00:0001.

Configuring an MLD snooping policy

Prerequisites

Before configuring 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 can pass the ports
- Determine the 802.1p precedence for MLD messages

Configuring an IPv6 multicast group filter

On an MLD snooping–enabled switch, the configuration of an IPv6 multicast group filter enables the service provider to define limits of multicast programs available to different users.

In an actual application, when a user requests a multicast program, the user's host initiates an MLD report. Upon receiving this report message, the switch compares the report against the configured ACL rule. If the port that received the report can join this IPv6 multicast group, the switch adds an entry for this port in the MLD snooping forwarding table. Otherwise, the switch drops this report message. Any IPv6 multicast data that fails the ACL verification is not sent to this port. In this way, the service provider can control the VOD programs provided for multicast users.

Configuring an IPv6 multicast group filter globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter MLD snooping view.	**mld-snooping**	—
3. Configure an IPv6 multicast group filter.	**group-policy** *acl6-number* [**vlan** *vlan-list*]	Required. By default, no IPv6 group filter is globally configured. That is, hosts in VLANs can join any valid multicast group.

Configuring an IPv6 multicast group filter on a port or a group of ports

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Configure an IPv6 multicast group filter.	**mld-snooping group-policy** *acl6-number* [**vlan** *vlan-list*]	Required. By default, no IPv6 group filter is configured on an interface. That is, hosts on the interface can join any valid multicast group.

Configuring IPv6 multicast source port filtering

With the IPv6 multicast source port filtering feature enabled on a port, the port can be connected with IPv6 multicast receivers only rather than with multicast sources, because the port will block all IPv6 multicast data packets while it permits multicast protocol packets to pass.

If this feature is disabled on a port, the port can be connected with both multicast sources and IPv6 multicast receivers.

Configuring IPv6 multicast source port filtering globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter MLD snooping view.	**mld-snooping**	—
3. Enable IPv6 multicast source port filtering.	**source-deny port** *interface-list*	Required. Defaults to disabled.

Configuring IPv6 multicast source port filtering on a port or a group of ports

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Enable IPv6 multicast source port filtering.	**mld-snooping source-deny**	Required. Defaults to disabled.

Configuring dropping unknown IPv6 multicast data

Unknown IPv6 multicast data refers to IPv6 multicast data for which no forwarding entries exist in the MLD snooping forwarding table. When the switch receives such IPv6 multicast traffic, one of the following occurs:

- With the function of dropping unknown IPv6 multicast data enabled, the switch drops all unknown IPv6 multicast data received.
- With the function of dropping unknown IPv6 multicast data disabled, the switch floods unknown IPv6 multicast data in the VLAN to which the unknown IPv6 multicast data belongs.

Follow these steps to enable dropping unknown IPv6 multicast data in a VLAN:

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Enable dropping unknown IPv6 multicast data.	**mld-snooping drop-unknown**	Required. Defaults to disabled.

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 directly connected with it. Thus, when multiple members that belong to an IPv6 multicast group exist on the Layer 2 switch, the Layer 3 device directly connected with it will receive duplicate MLD reports from these members.

With the MLD report suppression function enabled, within a query interval, the Layer 2 switch forwards only the first MLD report of an IPv6 group to the Layer 3 device. It will not forward the subsequent MLD reports from the same multicast group to the Layer 3 device. This helps reduce the number of packets that are transmitted over the network.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter MLD snooping view.	**mld-snooping**	—
3. Enable MLD report suppression.	**report-aggregation**	Optional. Enabled by default.

On an MLD snooping proxy, MLD 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.

Configuring maximum multicast groups that can be joined on a port

By configuring The maximum number of IPv6 multicast groups that can be joined on a port or a group of ports, you can limit the number of multicast programs available to VOD users, thus to control the traffic on the port.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—

To do...	Use the command...	Remarks
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Configure the maximum number of IPv6 multicast groups that can be joined on a port.	**mld-snooping group-limit** *limit* [**vlan** *vlan-list*]	Optional. 4000 by default for A5800 series Ethernet switches. 1000 by default for A5820X series Ethernet switches.

When the number of IPv6 multicast groups that can be joined on a port reaches the maximum number configured, the system deletes all the forwarding entries persistent to that port from the MLD snooping forwarding table, and the hosts on this port need to join IPv6 multicast groups again.

If you have configured static or simulated joining on a port, however, when the number of IPv6 multicast groups on the port exceeds the configured threshold, the system deletes all the forwarding entries persistent to that port from the MLD snooping forwarding table and applies the static or simulated joining again, until the number of IPv6 multicast groups joined by the port comes back within the configured threshold.

Configuring IPv6 multicast group replacement

Under some circumstances, the number of IPv6 multicast groups passing through a switch or port can exceed the upper limit. In addition, in some specific applications, an IPv6 multicast group newly joined on the switch must replace an existing IPv6 multicast group automatically. A typical example is "channel switching," where a user automatically switches from the current IPv6 multicast group to the new one by joining the new multicast group.

To address this, enable the IPv6 multicast group replacement function on the switch or certain ports. When the number of IPv6 multicast groups that a switch or a port has joined exceeds the limit, one of the following occurs:

- If the IPv6 multicast group replacement is enabled, the newly joined IPv6 multicast group automatically replaces an existing IPv6 multicast group with the lowest IPv6 address.
- If the IPv6 multicast group replacement is not enabled, new MLD reports will be automatically discarded.

Configuring IPv6 multicast group replacement globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter MLD snooping view.	**mld-snooping**	—
3. Enable IPv6 multicast group replacement.	**overflow-replace** [**vlan** *vlan-list*]	Required. Defaults to disabled.

Configuring IPv6 multicast group replacement on a port or a group of ports

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ethernet interface/Layer 2 aggregate interface view or port group view.	**interface** *interface-type interface-number* **port-group manual** *port-group-name*	Required. Use either approach.
3. Enable IPv6 multicast group replacement.	**mld-snooping overflow-replace** [**vlan** *vlan-list*]	Required. Defaults to disabled.

Be sure to configure the maximum number of IPv6 multicast groups allowed on a port (see) before enabling IPv6 multicast group replacement. Otherwise, the IPv6 multicast group replacement functionality will not take effect.

Configuring 802.1p precedence for MLD messages

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

Configuring 802.1p precedence for MLD messages globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter MLD snooping view.	**mld-snooping**	—
3. Configure 802.1p precedence for MLD Messages.	**dot1p-priority** *priority-number*	Required. The default 802.1p precedence for MLD messages is 0.

Configuring 802.1p precedence for MLD messages in a VLAN

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter VLAN view.	**vlan** *vlan-id*	—
3. Configure 802.1p precedence for MLD Messages.	**mld-snooping dot1p-priority** *priority-number*	Required. 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 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.

- Upon receiving an MLD report from a host, the access switch checks the IPv6 multicast group address and multicast source address carried in the report against 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.
- Upon receiving a done message from a host, the access switch matches the IPv6 multicast group and source addresses 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.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Create a user profile and enter its view.	**user-profile** *profile-name*	—
3. Configure a multicast user control policy.	**mld-snooping access-policy** *acl6-number*	Required. 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**	—
5. Enable the created user profile.	**user-profile** *profile-name* **enable**	Required. Not enabled by default.

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

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, while a multicast group filter is configured on a port to control only multicast joining but not leaving of users without authentication or authorization.

Displaying and maintaining MLD snooping

To do...	Use the command...	Remarks
Display MLD snooping group information	**display mld-snooping group** [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the statistics information of MLD messages learned by MLD snooping	**display mld-snooping statistics** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display IPv6 static multicast MAC address entries	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in user view
Remove dynamic group entries of a specified MLD snooping group or all MLD snooping groups	**reset mld-snooping group** { *ipv6-group-address* | **all** } [**vlan** *vlan-id*]	Available in user view

To do...	Use the command...	Remarks
Clear the statistics information of all kinds of MLD messages learned by MLD snooping	**reset mld-snooping statistics**	Available in user view

The **reset mld-snooping group** command works only on an MLD snooping–enabled VLAN, but not on a VLAN with MLD enabled on its VLAN interface.

The **reset mld-snooping group** command cannot remove the static group entries of MLD snooping groups.

For more information about **display mac-address multicast**, see *IP Multicast Command Reference*.

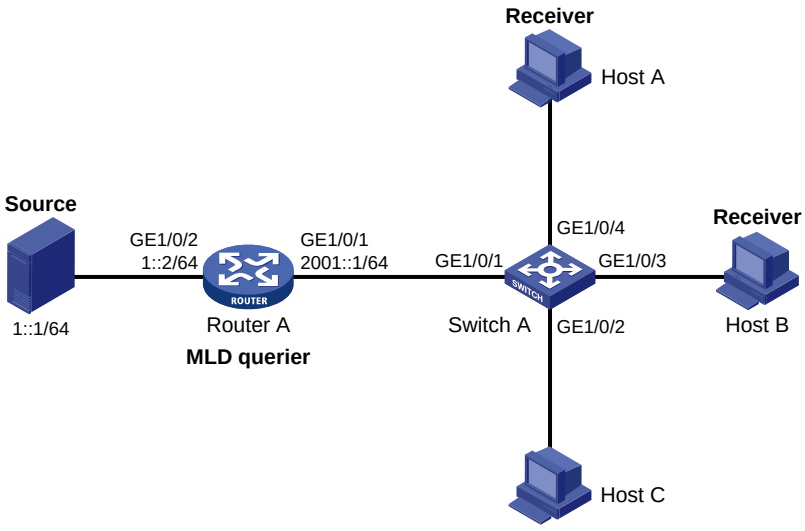
MLD snooping configuration examples

IPv6 group policy and simulated joining configuration example

Network requirements

- As shown in Figure 79, Router A connects to the IPv6 multicast source through GigabitEthernet 1/0/2 and to Switch A through GigabitEthernet 1/0/1. Router A is the MLD querier on the subnet.
- MLDv1 runs on Router A, MLDv1 snooping runs on Switch A, and Router A acts as the MLD querier on the subnet.
- The receivers, Host A and Host B, attached to Switch A 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.

Figure 79 Network diagram for IPv6 group policy simulated joining configuration



Procedure

1. Enable IPv6 forwarding and configure IPv6 addresses

Enable IPv6 forwarding and configure an IPv6 address and prefix length for each interface as shown in Figure 79. The detailed configuration steps are omitted.

2. Configure 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
```

4. Verify the configuration

Display the 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
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

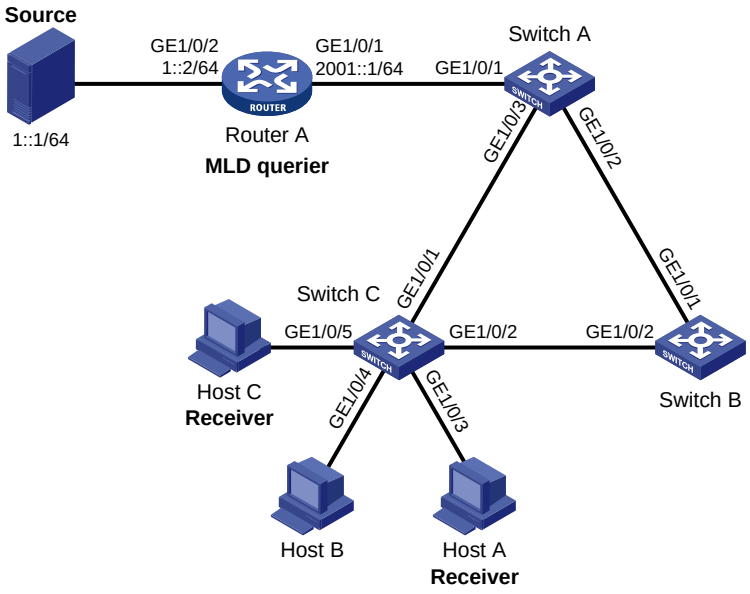
Network requirements

- As shown in Figure 80, Router A connects to an IPv6 multicast source (Source) through GigabitEthernet 1/0/2, and to Switch A through GigabitEthernet 1/0/1.
- MLDv1 runs on Router A, and MLDv1 snooping runs on Switch A, Switch B and Switch C, with Router A acting 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.
- You must configure GigabitEthernet 1/0/3 that connects Switch A to 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 gets blocked.

If no static router port is configured, when the path of Switch A—Switch B—Switch C gets 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 80 Figure Network diagram for static port configuration



Procedure

1. Enable IPv6 forwarding and configure IPv6 addresses

Enable IPv6 forwarding and configure an IPv6 address and prefix length for each interface as shown in Figure 80.

2. Configure 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
```

6. Verify the configuration

Display the 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
  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 the 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
  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
```

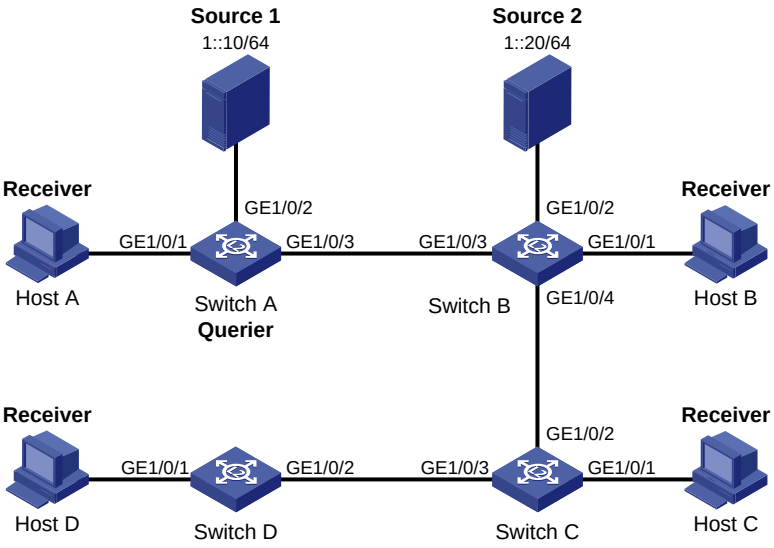
The output shows that GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 on Switch C have become static member ports for IPv6 multicast group FF1E::101.

MLD snooping querier configuration example

Network requirements

- As shown in Figure 81, 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, acts as the MLD 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.

Figure 81 Network diagram for MLD snooping querier 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
```

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

3. Verify 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 view the statistics information of these MLD messages received.

Display the MLD message statistics on Switch B.

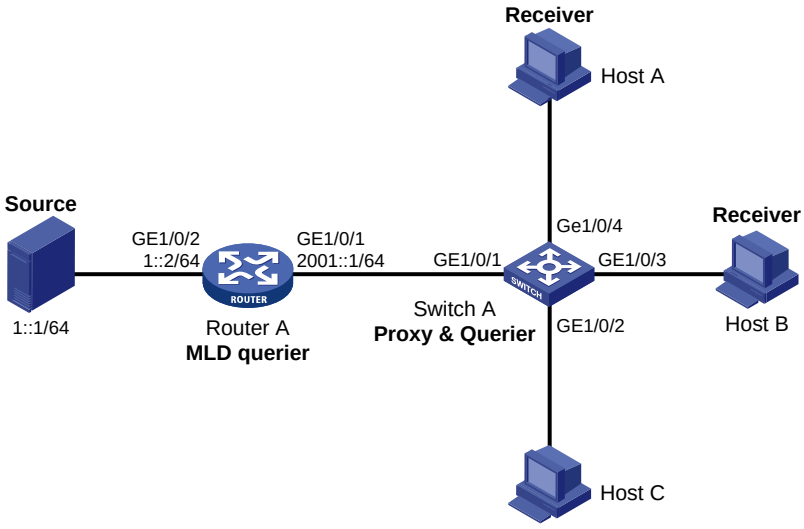
```
[SwitchB-vlan100] display mld-snooping statistics
  Received MLD general queries:3.
  Received MLDv1 specific queries:0.
  Received MLDv1 reports:12.
  Received MLD dones:0.
  Sent     MLDv1 specific queries:0.
  Received MLDv2 reports:0.
  Received MLDv2 reports with right and wrong records:0.
  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 82, Router A connects to an IPv6 multicast source through port GigabitEthernet 1/0/2, and to Switch A through port GigabitEthernet 1/0/1.
- Router A runs MLDv1 and Switch A runs MLDv1 snooping. Router A acts as an MLD querier.
- Configure MLD snooping proxying on Switch A, enabling the switch to forward MLD reports and done messages on behalf of attached hosts and to respond to MLD queries from Router A and forward the queries to the hosts on behalf of Router A.

Figure 82 Network diagram for MLD snooping proxying configuration



Procedure

1. Configure IPv6 addresses for interfaces

Configure an IP address and prefix length for each interface as shown in Figure 82. The configuration steps are out the scope of this document.

2. Configure 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
```

4. Verify 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 port GigabitEthernet 1/0/1 (a router port) to Router A. Use **display mld-snooping group** and **display mld group** 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
  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) ( 00:01:23 )
    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 1/0/3 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 **display mld-snooping group** 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).
```

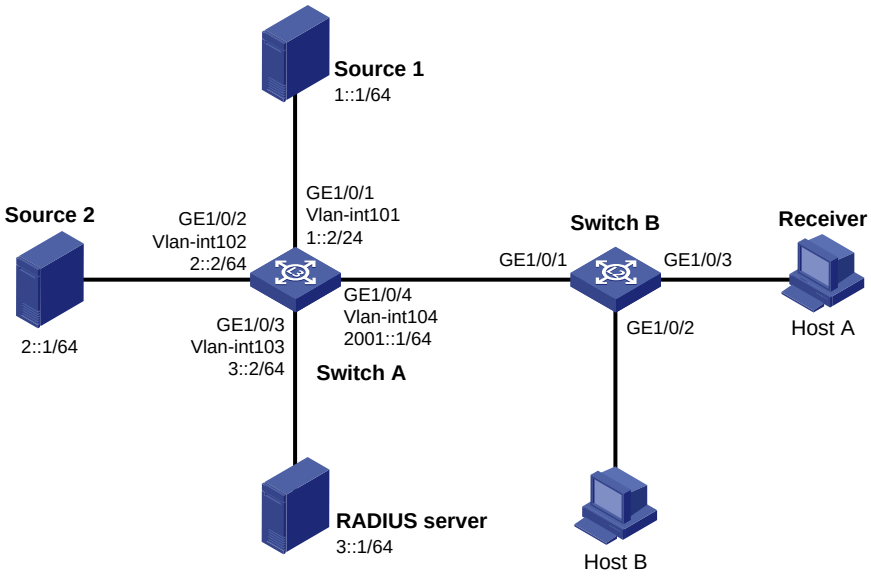
```
Total 1 MAC Group(s).
Port flags: D-Dynamic port, S-Static port, C-Copy port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 1 port(s).
          GE1/0/1                (D) ( 00:01:23 )
  IP group(s):the following ip group(s) match to one mac group.
    IP group address:FF1E::101
      (::, FF1E::101):
        Host port(s):total 1 port(s).
          GE1/0/4                (D)
  MAC group(s):
    MAC group address:3333-0000-0101
        Host port(s):total 1 port(s).
          GE1/0/4
```

IPv6 multicast source and user control policy configuration example

Network requirements

- As shown in Figure 83, Switch A is a Layer-3 switch. It connects to IPv6 multicast sources, Source 1 and Source 2, respectively through VLAN-interface 101 and VLAN-interface 102. It connects to the RADIUS server through VLAN-interface 103 and to the Layer-2 switch, Switch B, through VLAN-interface 104.
- Switch A runs MLDv1 and Switch B runs MLDv2 snooping. 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 83 Network diagram for IPv6 multicast source/user control policy configuration



Procedure

1. Configure IP addresses for interfaces

Enable IPv6 forwarding and configure an IP address and prefix length for each interface as shown in Figure 83. The configuration steps are omitted here.

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 ff1e::101 128
[SwitchA-acl6-adv-3001] quit
```

When configuring an IPv6 multicast source control policy, you need to apply an advanced IPv6 ACL to match both the multicast source address and destination address. Otherwise, multicast packets expected to be filtered out will still be delivered to the CPU for subsequent processing.

```
[SwitchA] traffic classifier classifier1
[SwitchA-classifier-classifier1] if-match acl ipv6 3001
[SwitchA-classifier-classifier1] quit
```

Do not reference any IPv4 ACL after an IPv6 ACL is referenced in classifier view. Otherwise, match errors will occur.

```
[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 Eth 1/2 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 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 MLD snooping.

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

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

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] 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 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 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.

5. Verify 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 **display mld-snooping group** to display information about MLD snooping groups. For example:

Display information about MLD snooping groups in VLAN 100 on Switch B.

```
[SwitchB] 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
  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 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 **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. It indicates that IPv6 multicast packets from Source 2 are blocked.

Troubleshooting MLD snooping

Switch fails in layer 2 multicast forwarding

Symptom

A switch fails to implement Layer 2 multicast forwarding.

Analysis

MLD snooping is not enabled.

Solution

1. Enter **display current-configuration** to view the running status of MLD snooping.
2. If MLD snooping is not enabled, use **mld-snooping** to enable MLD snooping globally, and then use **mld-snooping enable** to enable MLD snooping in VLAN view.
3. If MLD snooping is disabled only for the corresponding VLAN, just use **mld-snooping enable** 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 **display acl ipv6** to view the configured IPv6 ACL rule. Be sure that the IPv6 ACL rule conforms to the IPv6 multicast group policy to be implemented.
2. Use **display this** in MLD snooping view or the corresponding interface view to determine whether the correct IPv6 multicast group policy has been applied. If not, use **group-policy** or **mld-snooping group-policy** to apply the correct IPv6 multicast group policy.
3. Use **display current-configuration** to determine whether the function of dropping unknown IPv6 multicast data is enabled. If not, use **mld-snooping drop-unknown** 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 switch processes IPv6 multicast protocol messages differently under different conditions:

- If only MLD is enabled, or both MLD and IPv6 PIM are enabled on the switch, the switch:
  - Maintains dynamic member ports or dynamic router ports according to MLD packets.
  - Maintains dynamic router ports according to IPv6 PIM hello packets.
- In only IPv6 PIM is enabled on the switch:
  - The switch broadcasts MLD messages as unknown messages in the VLAN.
  - Upon receiving an IPv6 PIM hello message, the switch will maintain the corresponding dynamic router port.
- When MLD is disabled on the switch:
  - 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 without deleting its dynamic router ports.

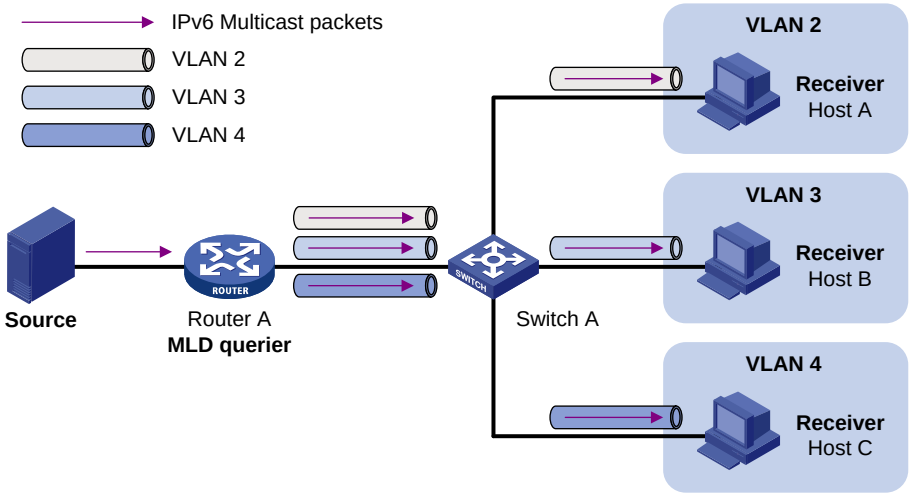
On a switch with Layer-3 IPv6 multicast routing enabled, use **display mld group port-info** to view Layer-2 port information. For more information about **display mld group port-info**, see *IP Multicast Command Reference*.

- When IPv6 PIM is disabled on the switch:
  - 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 multicast VLAN

As shown in Figure 84, in the traditional IPv6 multicast programs-on-demand mode, when 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 84 Multicast transmission without IPv6 multicast VLAN



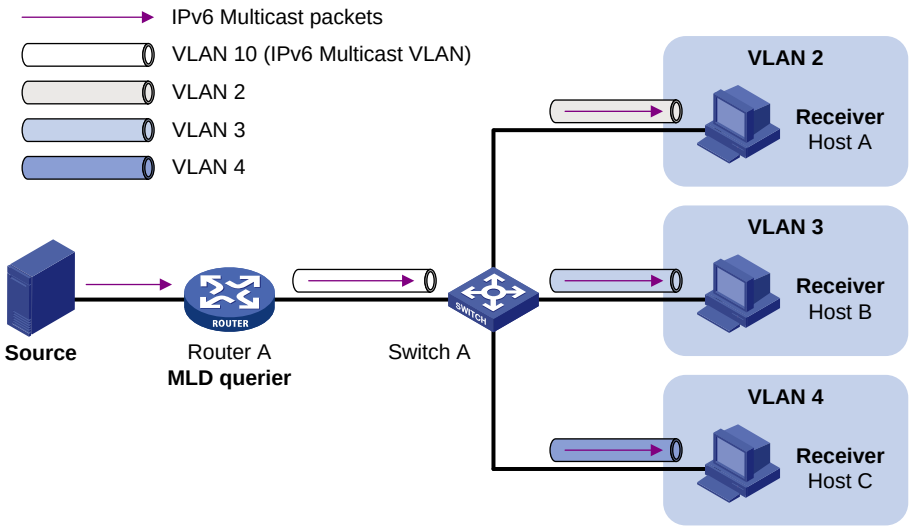
The IPv6 multicast VLAN feature configured on the Layer 2 device is the solution to this issue. With the IPv6 multicast VLAN feature, the Layer 3 device needs to replicate the multicast traffic only in the IPv6 multicast VLAN instead of making a separate copy of the multicast traffic in each user VLAN. This saves network bandwidth and lessens the burden on the Layer 3 device.

The IPv6 multicast VLAN feature can be implemented in two approaches, as described below:

Sub-VLAN-based IPv6 multicast VLAN

As shown in Figure 85, Host A, Host B, and Host C are in three different user VLANs. On Switch A, configure VLAN 10 as an IPv6 multicast VLAN, configure all user VLANs as sub-VLANs of this IPv6 multicast VLAN, and enable MLD snooping in the IPv6 multicast VLAN.

Figure 85 Sub-VLAN-based IPv6 multicast VLAN

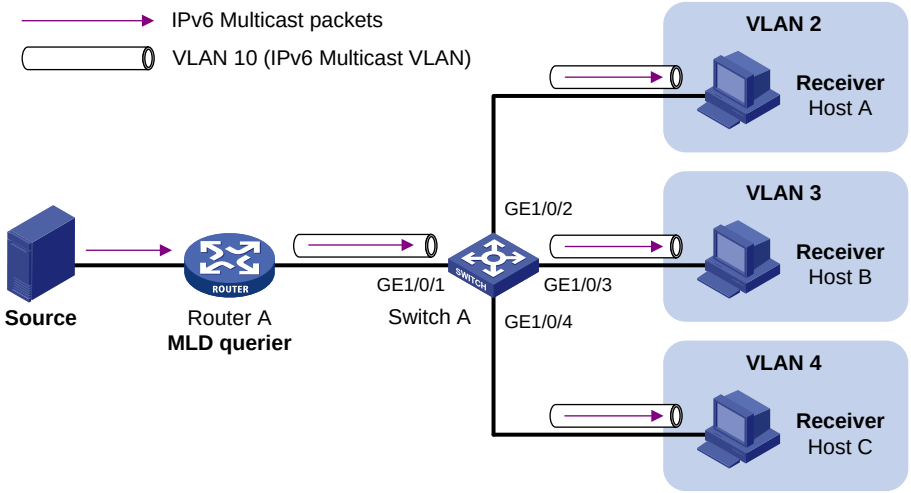


After the configuration, MLD snooping manages router ports in the IPv6 multicast VLAN and member ports in the sub-VLANs. When forwarding multicast data to Switch A, Router A needs to send only one copy of multicast traffic to Switch A in the IPv6 multicast VLAN, and Switch A distributes the traffic to the IPv6 multicast VLAN's sub-VLANs that contain receivers.

Port-based IPv6 multicast VLAN

As shown in Figure 86, Host A, Host B and Host C are in three different user VLANs. All the user ports are hybrid ports. On Switch A, configure VLAN 10 as an IPv6 multicast VLAN, assign all user ports to this IPv6 multicast VLAN, and enable MLD snooping in the IPv6 multicast VLAN and all user VLANs.

Figure 86 Port-based IPv6 multicast VLAN



After the configuration, upon receiving an MLD message on a user port, Switch A 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 forwarding multicast data to Switch A, Router A needs to send only one copy of multicast traffic to Switch A in the IPv6 multicast VLAN, and Switch A distributes the traffic to all member ports in the IPv6 multicast VLAN.

For more information about MLD Snooping, router ports, and member ports, see *IP Multicast Configuration Guide*.

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

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 IPv6 sub-VLAN-based IPv6 multicast VLAN

Prerequisites

Before configuring sub-VLAN-based IPv6 multicast VLAN, complete the following tasks:

- Create VLANs as required
- Enable MLD snooping in the VLAN to be configured as an IPv6 multicast VLAN

Configuring sub-VLAN-based IPv6 multicast VLAN

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 do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.	**multicast-vlan ipv6** *vlan-id*	Required. No IPv6 multicast VLAN configured by default.
3. Configure the specified VLAN(s) as sub-VLAN(s) of the IPv6 multicast VLAN.	**subvlan** vlan-list	Required. By default, an IPv6 multicast VLAN has no sub-VLANs.

You cannot configure 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 sub-VLANs of another IPv6 multicast VLAN.

Configuring port-based IPv6 multicast VLAN

When configuring 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 of the Ethernet, or Layer 2 aggregate interface type.

Configurations made in Ethernet interface view is effective only for the current port; configurations made in Layer 2 aggregate interface view are effective only for the current interface; configurations made in port group view are effective for all the ports in the current port group.

Prerequisites

Before configuring port-based IPv6 multicast VLAN, complete the following tasks:

- 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

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.

Configure the user ports to permit packets of the IPv6 multicast VLAN to pass and untag the packets. Thus, upon 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view or port group view.	**interface** interface-type interface-number	Required. Use either approach.
	port-group manual *port-group-name*	
3. Configure the user port link type as hybrid.	**port link-type hybrid**	Required. Access by default.
4. Specify the user VLAN that comprises the current user port(s) as the default VLAN.	**port hybrid pvid vlan** *vlan-id*	Required. 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** *vlan-id-list* { **tagged** | **untagged** }	Required. By default, a hybrid port permits only packets of VLAN 1 to pass.

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

Configuring IPv6 multicast VLAN ports

In this approach, you need to configure a VLAN as an IPv6 multicast VLAN and then assign user ports to this IPv6 multicast VLAN by either adding the user ports in the IPv6 multicast VLAN or specifying the IPv6 multicast VLAN on the user ports. These two methods give the same result.

Configure IPv6 multicast VLAN ports in IPv6 multicast VLAN view

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—

To do...	Use the command...	Remarks
2. Configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.	**multicast-vlan ipv6** *vlan-id*	Required. No IPv6 multicast VLAN configured by default.
3. Assign port(s) to the IPv6 multicast VLAN.	**port** interface-list	Required. By default, an IPv6 multicast VLAN has no ports.

Configure IPv6 multicast VLAN ports in interface view or port group view

To do...	Use this command...	Remarks
1. Enter system view	**system-view**	—
2. Configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.	**multicast-vlan ipv6** *vlan-id*	Required. Not an IPv6 multicast VLAN by default.
3. Return to system view.	**quit**	—
4. Enter interface view or port group view.	**interface** interface-type interface-number **port-group manual** *port-group-name*	Required. Use either command.
5. Configure the port(s) as port(s) of the IPv6 multicast VLAN.	**port multicast-vlan ipv6** *vlan-id*	Required. By default, a user port does not belong to any IPv6 multicast VLAN.

You cannot configure 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.

Displaying and maintaining IPv6 multicast VLAN

To do...	Use the command...	Remarks
Display information about an IPv6 multicast VLAN	**display multicast-vlan ipv6** [*vlan-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

IPv6 multicast VLAN configuration examples

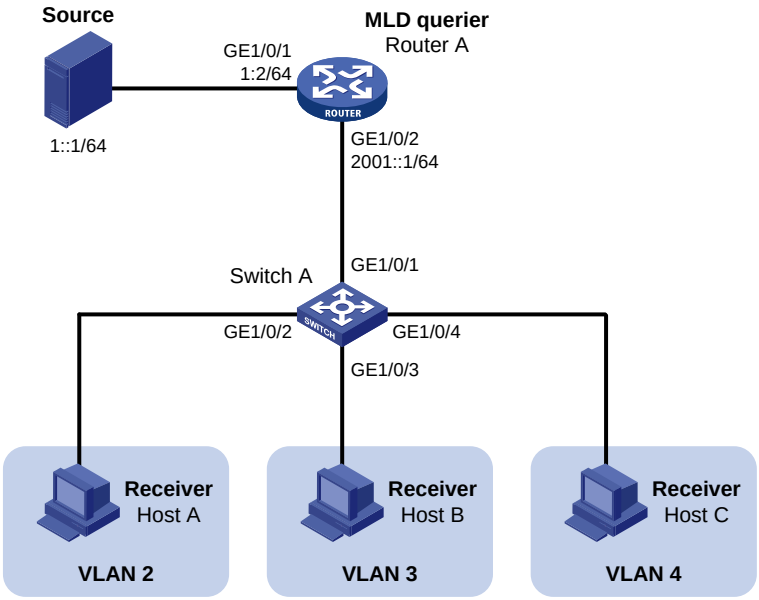
Sub-VLAN-based multicast VLAN configuration example

Network requirements

- As shown in Figure 87, Router A connects to an IPv6 multicast source through GigabitEthernet 1/0/1 and to Switch A, through GigabitEthernet 1/0/2.
- MLDv1 runs on Router A, and MLD snooping runs on Switch A. Router A is the MLD querier.

- Switch A's GigabitEthernet 1/0/1 belongs to VLAN 10, GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 belong to VLAN 2 through VLAN 4 respectively, and Host A through Host C are attached to GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 of Switch A.
- The IPv6 multicast source sends IPv6 multicast data to the IPv6 multicast group FF1E::101. Host A, Host B, and Host C are receivers of the IPv6 multicast group.
- Configure the sub-VLAN-based IPv6 multicast VLAN feature 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 87 Network diagram for sub-VLAN-based IPv6 multicast VLAN configuration



Procedure

1. Enable IPv6 forwarding and configure IPv6 addresses

Enable IPv6 forwarding on each device and configure an IPv6 address and address prefix for each interface as shown in Figure 87. The detailed configuration steps are omitted here.

2. Configure 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 and assign GigabitEthernet 1/0/2 to this VLAN.

```
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/2
[SwitchA-vlan2] quit
```

The configuration for VLAN 3 and VLAN 4 is similar to the configuration for VLAN 2.

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 4 as its sub-VLANs.

```
[SwitchA] multicast-vlan ipv6 10
[SwitchA-ipv6-mvlan-10] subvlan 2 to 4
[SwitchA-ipv6-mvlan-10] quit
```

4. Verify 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 2-4
   port list:
    no port
```

View the MLD snooping IPv6 multicast group information on Switch A.

```
[SwitchA] display mld-snooping group
  Total 4 IP Group(s).
  Total 4 IP Source(s).
  Total 4 MAC Group(s).
  Port flags: D-Dynamic port, S-Static port, C-Copy 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).
          GE1/0/3                (D)
  MAC group(s):
    MAC group address:3333-0000-0101
        Host port(s):total 1 port(s).
          GE1/0/3
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).
          GE1/0/4                (D)
  MAC group(s):
    MAC group address:3333-0000-0101
        Host port(s):total 1 port(s).
          GE1/0/4
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).
```

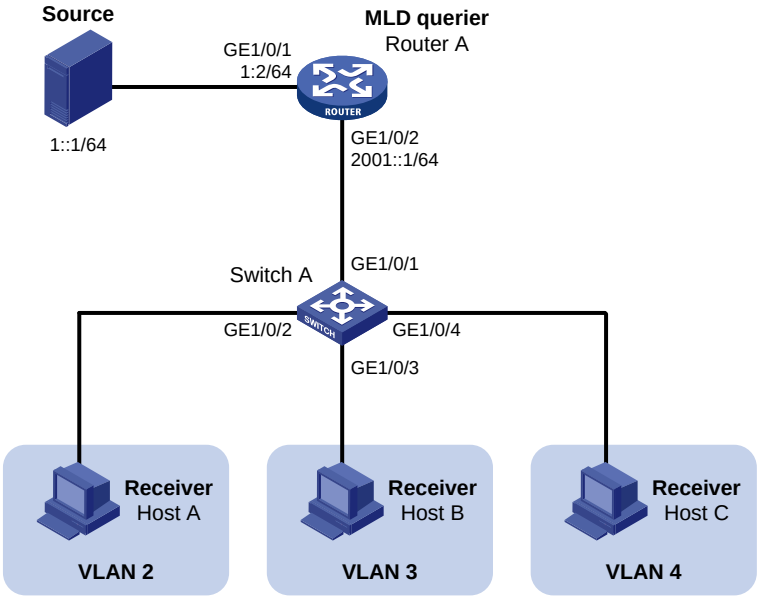
The output shows that MLD snooping is maintaining the router port in the IPv6 multicast VLAN (VLAN 10) and the member ports in the sub-VLANs (VLAN 2 through VLAN 4).

Port-based multicast VLAN configuration example

Network requirements

- As shown in Figure 88, Router A connects to an IPv6 multicast source (Source) through GigabitEthernet 1/0/1, and to Switch A through GigabitEthernet 1/0/2.
- MLDv1 runs on Router A. MLDv1 snooping runs on Switch A. Router A acts as the MLD querier.
- Switch A's GigabitEthernet 1/0/1 belongs to VLAN 10, GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 belong to VLAN 2 through VLAN 4 respectively, and Host A through Host C are attached to GigabitEthernet 1/0/2 through GigabitEthernet 1/0/4 of Switch A.
- 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.
- Configure the port-based IPv6 multicast VLAN feature so that Router A just sends IPv6 multicast data to Switch A through the IPv6 multicast VLAN and Switch A forward the IPv6 multicast data to the receivers that belong to different user VLANs.

Figure 88 Network diagram for port-based IPv6 multicast VLAN configuration



Procedure

1. Enable IPv6 forwarding and configure IPv6 addresses

Enable IPv6 forwarding on each device and configure the IPv6 address and address prefix for each interface as shown in Figure 88. The detailed configuration steps are omitted here.

2. Configure 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. The detailed configuration steps are omitted.

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. The detailed configuration steps are omitted.

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
```

4. Verify the configuration

View 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
```

View 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
  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

Interface view mentioned in this chapter can be VLAN interface view or Layer 3 Ethernet interface view. Layer 3 Ethernet interfaces refer to Ethernet interfaces configured to operate in route mode. To switch the operating mode of an Ethernet port, see *Layer 2 - LAN Switching Configuration Guide*.

- In IPv6 multicast implementations, tables implement multicast routing and forwarding. each IPv6 multicast routing protocol has its own multicast routing table, such as the IPv6 PIM routing table.
- The multicast routing information about different IPv6 multicast routing protocols forms a general IPv6 multicast routing 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 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.

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 RPF verification mechanism to ensure IPv6 multicast data delivery along the correct path. the RPF verification mechanism also helps avoid data loops.

RPF check process

The basis for an RPF verification is an IPv6 unicast route or an IPv6 MBGP route.

- An IPv6 unicast routing table contains the shortest path to each destination subnet;
- An IPv6 MBGP routing table contains IPv6 multicast routing information.

When performing an RPF verification, a router 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 an optimal route from the IPv6 unicast routing table and IPv6 MBGP routing table respectively.
   - 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. It uses 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 the two. If these two routes have the same prefix length, the router selects the route with a higher priority. If these two 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 two routes have the same priority, the router selects the IPv6 MBGP route as the RPF route.
3. The term *packet source* can mean different things in different situations.
   - For a packet that is traveling along the SPT from the multicast source to the receivers or the RP, the packet source for RPF verification is the multicast source.
   - For a packet that is traveling along the RPT from the RP to the receivers, the packet source for RPF verification is the RP.
   - For a bootstrap message from the BSR, the packet source for RPF verification is the BSR.

For more information about the concepts of SPT, RPT, RP, and BSR, see *IP Multicast Configuration Guide*.

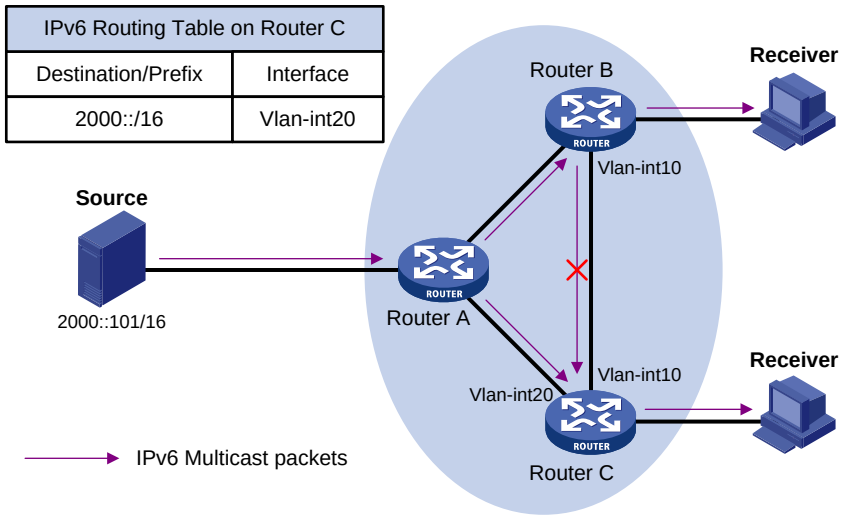
Implementation of the RPF check in IPv6 multicast

Implementing an RPF verification 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. Upon receiving an (S, G) IPv6 multicast packet, the router first searches its IPv6 multicast forwarding table.

- If the corresponding (S, G) entry does not exist in the IPv6 multicast forwarding table, the packet undergoes an RPF verification. 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 on which the packet arrived is the RPF interface, the RPF verification succeeds and the router forwards the packet to all the outgoing interfaces.
- If the interface on which the packet arrived is not the RPF interface, the RPF verification fails and the router discards the packet.
- If the corresponding (S, G) entry exists, and the interface on which the packet arrived is the incoming interface, the router forwards the packet to all the outgoing interfaces.
- If the corresponding (S, G) entry exists, but the interface on which the packet arrived is not the incoming interface in the IPv6 multicast forwarding table, the IPv6 multicast packet undergoes an RPF verification.
- If the RPF interface is the incoming interface of the (S, G) entry, this means 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, this means 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 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 89. The IPv6 multicast forwarding table on Router C contains the (S, G) entry, with VLAN-interface 20 as the RPF interface.

Figure 89 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 verification 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 verification fails and the packet is discarded.

Enabling IPv6 multicast routing

Before configuring any Layer 3 IPv6 multicast functionality, you must enable IPv6 multicast routing.

To do…	Use the Command…	Remarks
1. Enter system view.	**system-view**	—
2. Enable IPv6 multicast routing.	**multicast ipv6 routing-enable**	Required. Defaults to disabled.

Configuring IPv6 multicast routing and forwarding

Prerequisites

Before configuring 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 forwarding

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

."

Configuring per-source or per-source-and-group load splitting can optimize the traffic delivery when multiple IPv6 multicast data streams are handled.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
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. Defaults to disabled.

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 define an IPv6 multicast forwarding range by:

- Specifying boundary interfaces, which form a closed IPv6 multicast forwarding area.
- Setting the minimum hop limit value required for an IPv6 multicast packet to be forwarded.

Setting the minimum hop limit is not supported on A5820X&A5800 series switches.

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. After you configure an IPv6 multicast boundary on an interface, the interface can no longer forward IPv6 multicast packets (including those sent from the local device) or receive IPv6 multicast packets.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure an IPv6 multicast forwarding boundary.	**multicast ipv6 boundary** { *ipv6-group-address prefix-length* | **scope** { *scope-id* | **admin-local** | **global** | **organization-local** | **site-local** } }	Required. 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 memory and decrease switch 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 will not be immediately deleted. Instead, the IPv6 multicast routing protocol that is running on the switch delete them. The switch will no longer install new IPv6 multicast forwarding entries until the number of existing IPv6 multicast forwarding entries comes down below the configured value.

When forwarding IPv6 multicast traffic, the switch replicates a copy of the IPv6 multicast traffic for each downstream node and forwards the traffic, and thus each of these downstream nodes forms a branch of the IPv6 multicast distribution tree. You can configure the maximum number of downstream nodes (namely, 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 will not be deleted immediately. Instead, the IPv6 multicast routing protocol must delete them. The switch will no longer install new IPv6 multicast forwarding entries for newly added downstream nodes until the number of existing downstream nodes comes down below the configured value.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Configure the maximum number of entries in the IPv6 multicast forwarding table.	**multicast ipv6 forwarding-table route-limit** *limit*	Optional. • 4000 by default for A5800 Switch Series. • 1000 by default for A5820X Switch Series.
3. Configure the maximum number of downstream nodes for a single IPv6 multicast forwarding entry.	**multicast ipv6 forwarding-table downstream-limit** *limit*	Optional. Defaults to 128.

On an A5800 series Ethernet switch:

- Without MPLS enabled, the switch can have up to 4000 IPv6 multicast forwarding entries. With MPLS enabled, the switch can have up to 3000 IPv6 multicast forwarding entries.
- If the number of the IPv6 multicast forwarding entries on the switch is more than 3000, you cannot enable MPLS on the switch.

Displaying and maintaining IPv6 multicast routing and forwarding

To do...	Use the command...	Remarks
Display the IPv6 multicast boundary information.	**display multicast ipv6 boundary** { **group** [*ipv6-group-address* [*prefix-length*]] | **scope** [*scope-id*] } [**interface** *interface-type interface-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

To do...	Use the command...	Remarks
Display the information of the IPv6 multicast forwarding table.	**display multicast ipv6 forwarding-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } } | **statistics** | **slot** *slot-number*] * [**port-info**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the DF information of the IPv6 multicast forwarding table.	**display multicast ipv6 forwarding-table df-info** [*rp-address*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the information of the IPv6 multicast routing table.	**display multicast ipv6 routing-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } }] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the RPF route information of the specified IPv6 multicast source.	**display multicast ipv6 rpf-info** *ipv6-source-address* [*ipv6-group-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Clear forwarding entries from the IPv6 multicast forwarding table.	**reset multicast ipv6 forwarding-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }	Available in user view.
Clear routing entries from the IPv6 multicast routing table.	**reset multicast ipv6 routing-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }	Available in user view.

The **reset** command clears the information in the IPv6 multicast routing table or the multicast forwarding table, and thus may cause transmission failure of IPv6 multicast information.

When a routing entry is deleted from the IPv6 multicast routing table, the corresponding forwarding entry will also be deleted from the IPv6 multicast forwarding table.

When a forwarding entry is deleted from the IPv6 multicast forwarding table, the corresponding routing entry will also be deleted from the IPv6 multicast routing table.

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, **source-policy** 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 **display current-configuration** 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 address of the IPv6 multicast packets and the IPv6 multicast group address can both match the IPv6 ACL rule.
2. Evaluate the configuration of the multicast filter. Use **display current-configuration** to view the configuration of the IPv6 multicast filter, and change the IPv6 ACL rule used in **source-policy** so that the source address of the IPv6 multicast packets and the IPv6 multicast group address can both match the IPv6 ACL rule.

Configuring MLD

An IPv6 router uses MLD to discover the presence of multicast listeners on the directly attached subnets. Multicast listeners are nodes that 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 that are running MLD use an IPv6 unicast link-local address as the source address to send MLD messages. MLD messages are ICMPv6 messages. All MLD messages are confined to the local subnet, with a hop count of 1.

Interface view mentioned in this chapter can be VLAN interface view or Layer 3 Ethernet interface view. Layer 3 Ethernet interfaces refer to Ethernet interfaces configured to operate in route mode. To switch the operating mode of an Ethernet port, see *Layer 2 - LAN Switching Configuration Guide*.

MLD versions

The following MLD versions are available:

- 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 ASM model. In addition, you can directly deploy MLDv2 to implement the SSM model, while MLDv1 needs to work with the MLD SSM mapping function to implement SSM service.

For more information about the ASM and SSM models, see *IP Multicast Configuration Guide*.

Understanding MLDv1

MLDv1 implements IPv6 multicast listener management based on the query/response mechanism.

MLD querier election

Of multiple IPv6 multicast routers on the same subnet, all the routers can monitor MLD listener report messages (often called "reports") from hosts, but only one router is needed for sending MLD query messages (often called "queries"). A querier election mechanism determines which router will act as the MLD querier on the subnet.

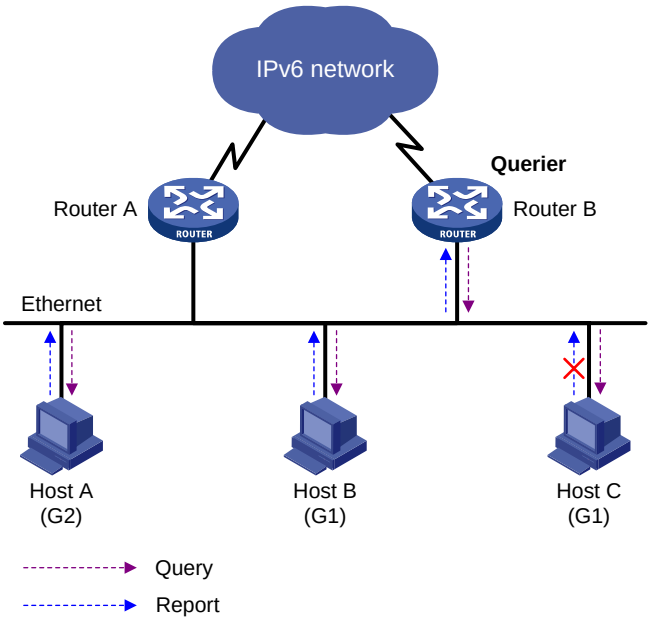
Initially, every MLD router assumes itself as the querier and sends MLD general query messages (often called "general queries") to all hosts and routers on the local subnet. The destination address is FF02::1.

Upon identifying 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.

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 the querier has timed out and initiates a new querier election process.

Joining an IPv6 multicast group

Figure 90 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 90. The following process describes how the hosts join the IPv6 multicast groups and how the MLD querier (Router B in Figure 90) maintains the IPv6 multicast group memberships:

1. The hosts send unsolicited MLD reports to the addresses of the IPv6 multicast groups that they 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. Upon 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. Upon 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 determined that at least one host on the local subnet is available for G1. This mechanism, called the "MLD report suppression", helps reduce traffic on the local subnet.
4. At the same time, because Host A is available for G2, it sends a report to the IPv6 multicast group address of G2.
5. Through the query/report process, the MLD routers discover that members of G1 and G2 are attached to the local subnet. The IPv6 multicast routing protocol (IPv6 PIM, for example) 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 process occurs:

1. The host sends an MLD done message to all IPv6 multicast routers on the local subnet. The destination address is FF02::2
2. Upon 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 that is 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 available for IPv6 multicast traffic addressed to that group and will stop maintaining the memberships of the group.

Understanding MLDv2

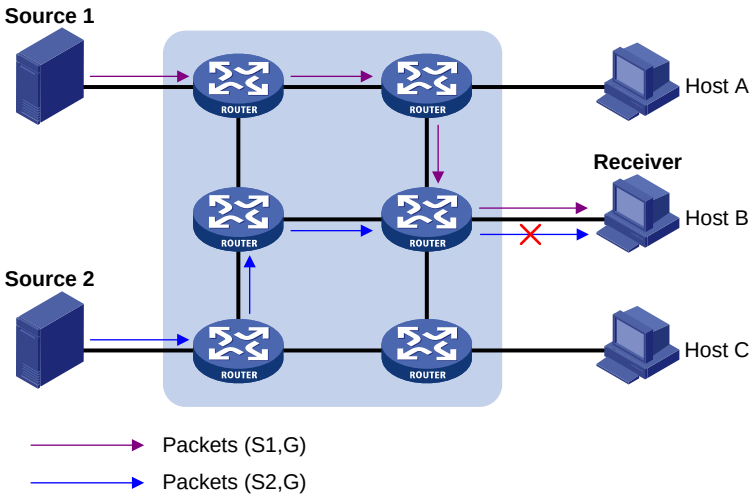
IPv6 multicast group filtering

MLDv2 has introduced IPv6 multicast source filtering modes (Include and Exclude), so that a host can specify a list of IPv6 multicast sources that it expects or does not expect IPv6 multicast data from when it joins an IPv6 multicast group.

- 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 91, 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 available for the IPv6 multicast data that Source 1 sends to G but not for the data from Source 2.

Figure 91 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 availability for 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:

- **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 timer and source timer. The filter timer (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 Message types

The following descriptions are based on MLDv2 messages.

MLD query message

An MLD querier identifies the multicast monitoring state of neighbor interfaces by sending MLD query messages. In Figure 92, the darker area shows the format of an MLDv1 message.

Figure 92 Format of MLDv2 query message

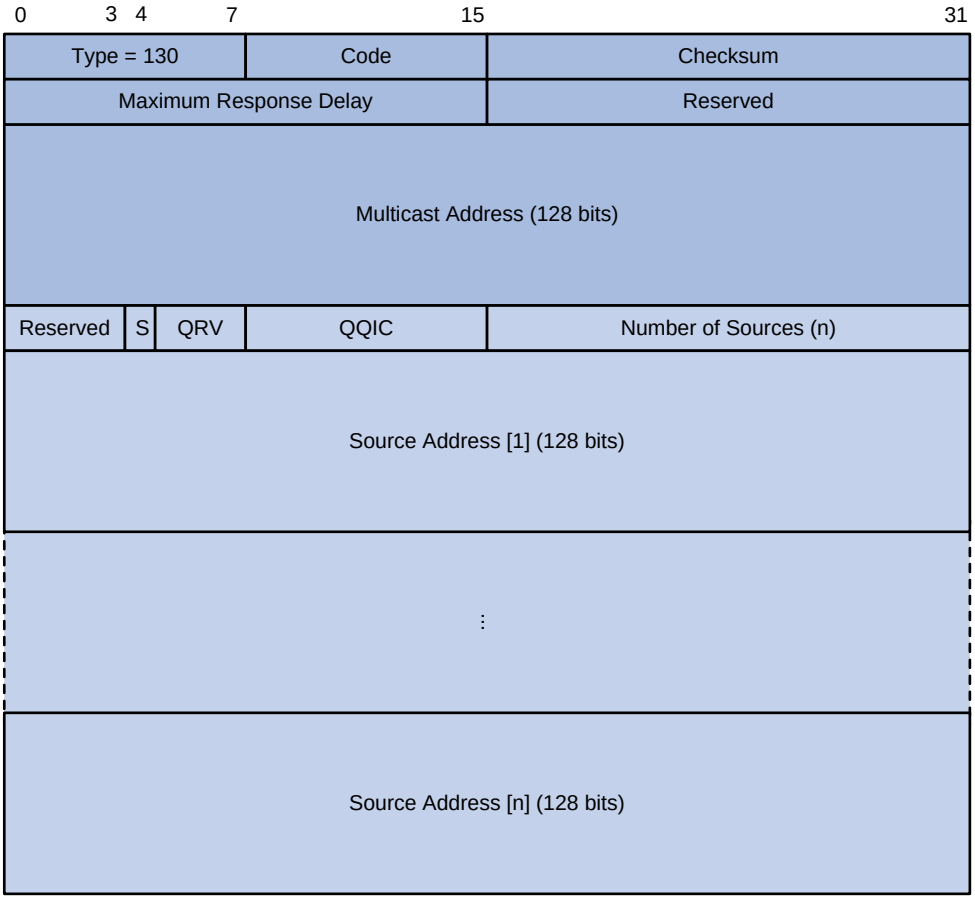


Table 15 Description on fields in an MLDv2 query message

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
Multicast Address	• 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

Field	Description
Number of Sources	• 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 represents the number of multicast source addresses.)

MLD report message

A host sends an MLD report message to report the current multicast monitoring state.

Figure 93 Format of MLDv2 report message

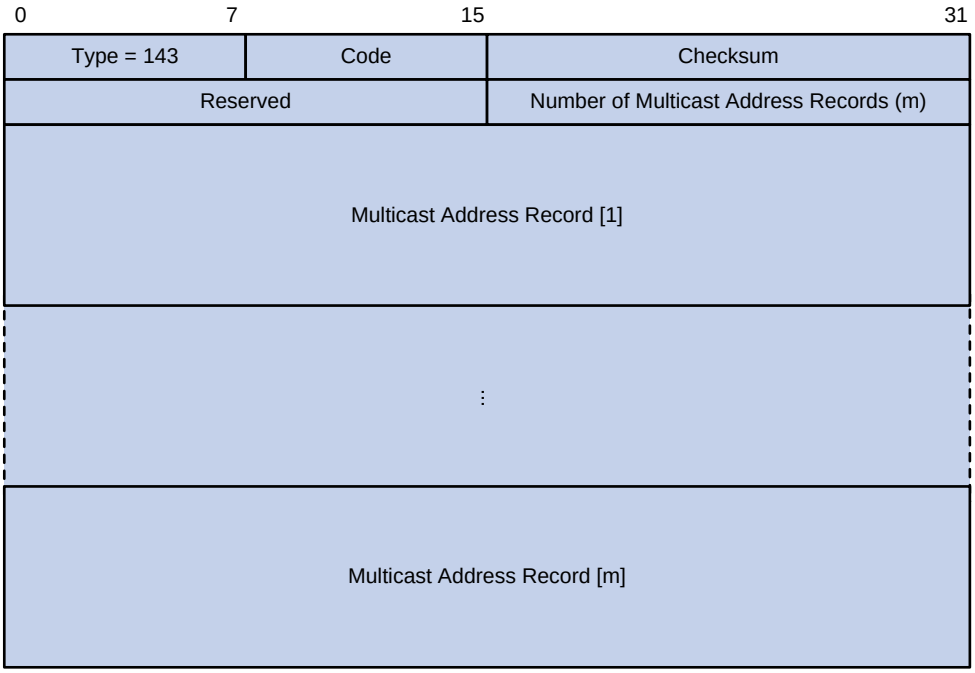


Table 16 Description on fields in an MLDv2 report message

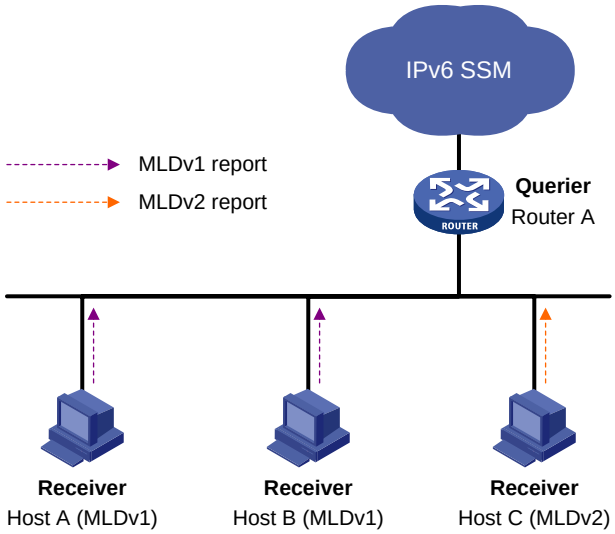
Field	Description
Type = 143	Message type. For a report message, this field is set to 143.
Reserved	The Reserved fields are set to 0 on transmission and ignored on reception.
Checksum	Standard IPv6 checksum
Number of Multicast Address Records	This field indicates how many IPv6 multicast address records 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 represents the number of IPv6 multicast address records.

MLD SSM mapping

You can use the MLD SSM mapping feature 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 a host that is running MLDv2 joins a multicast group, it can explicitly specify one or more multicast sources in its MLDv2 report.
- A host that is running MLDv1 cannot specify multicast source addresses in its MLDv1 report. In this case, you must configure the MLD SSM mapping feature to translate the (*, G) information in the MLDv1 report into (G, INCLUDE, (S1, S2...)) information.

Figure 94 Network diagram for MLD SSM mapping



As shown in Figure 94, on an IPv6 SSM network, Host A and Host B are running MLDv1 and Host C is running MLDv2. To provide SSM service for all the hosts while it is infeasible to run MLDv2 on 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 evaluates 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 that correspond to the IPv6 multicast group G have been configured 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.

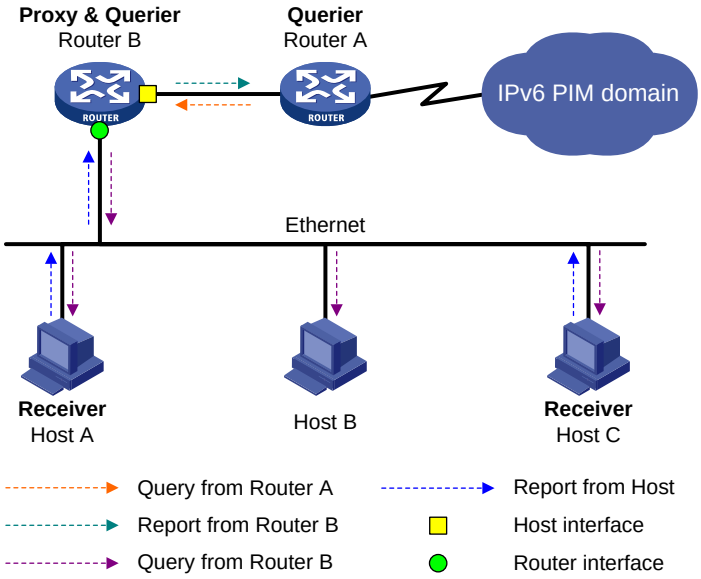
The MLD SSM mapping feature does not process MLDv2 reports.

For more information about the IPv6 SSM group range, see *IP Multicast Configuration Guide*.

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 device. Instead, you can configure MLD proxying on the boundary device. 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 95 Network diagram for MLD proxying



As shown in Figure 95, an MLD proxy device defines 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. Therefore, it 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. Therefore, it 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")*

Configurations performed in MLD view are globally effective, while configurations performed in interface view are effective on the current interface only.

If no configuration is performed in interface view, the global configurations performed in MLD view will apply to that interface. Configurations performed in interface view take precedence over those performed in MLD view.

Configuring basic functions of MLD

Prerequisites

Before configuring the basic functions of MLD, complete the following tasks:

- Configure any 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 can be joined on an interface

Enabling MLD

Enable MLD on the interface where IPv6 multicast group memberships are created and maintained. You must perform this task to configure the basic functions of MLD. All other tasks are optional.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enable IPv6 multicast routing.	**multicast ipv6 routing-enable**	Required. Disable by default.
3. Enter interface view.	**interface** *interface-type interface-number*	—
4. Enable MLD.	**mld enable**	Required. Defaults to disabled.

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

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter MLD view.	**mld**	—
3. Configure an MLD version globally.	**version** *version-number*	Optional. MLDv1 by default.

Configuring an MLD version on an interface

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure an MLD version on the interface.	**mld version** *version-number*	Optional. MLDv1 by default.

Configuring static joining

After you configure an interface as a static member of an IPv6 multicast group or an IPv6 multicast source and group, the interface 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.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure a static member of an IPv6 multicast group or an IPv6 multicast source and group.	**mld static-group** *ipv6-group-address* [**source** *ipv6-source-address*]	Required. By default, an interface is not a static member of any IPv6 multicast group or IPv6 multicast source and group.

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 *IP Multicast Configuration Guide*.

As a static member of an IPv6 multicast group or an IPv6 multicast source and group, an interface does not respond to the queries from the MLD querier. Nor does it send an unsolicited MLD membership report or an MLD done message when it joins or leaves an IPv6 multicast group or an IPv6 source and group. In other words, the interface will not become a real member of the IPv6 multicast group or the IPv6 multicast and source group.

Configuring an ipv6 multicast group filter

To restrict the hosts on the network attached to an interface from joining certain IPv6 multicast groups, set an IPv6 ACL rule on the interface so that the interface maintains only the IPv6 multicast groups matching the criteria.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure an IPv6 multicast group filter.	**mld group-policy** *acl6-number* [*version-number*]	Required. By default, no IPv6 group filter is configured on the interface. That is, hosts on the current interface can join any valid multicast group.

Configuring the maximum number of IPv6 multicast groups on an interface

You can configure the allowed maximum number of the IPv6 multicast groups on an interface to flexibly control the number of IPv6 multicast groups the interface can join.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure the maximum number of IPv6 multicast groups that the interface can join.	**mld group-limit** *limit*	Required. • 4000 by default for A5800 Switch Series. • 1000 by default for A5820X Switch Series.

This configuration takes effect for dynamically joined IPv6 multicast groups but not the statically configured multicast groups.

Adjusting MLD performance

The following points apply to the configuration tasks described in this section:

- Configurations performed in MLD view are globally effective, while configurations performed in interface view are effective on the current interface only.
- If the same function or parameter is configured in both PIM view and interface view, the configuration performed in interface view has priority, regardless of the configuration sequence.

Prerequisites

Before adjusting MLD performance, complete the following tasks:

- Configure any IPv6 unicast routing protocol so that all devices in the domain can be interoperable at the network layer.
- Configure basic functions of MLD.
- 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

Configuring MLD message options

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:

- By default, in consideration of compatibility, the device does not evaluate the Router-Alert option. That is, it processes all received MLD messages. In this case, the device passes MLD messages to the upper layer protocol for processing, 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 the Router-Alert option for MLD messages globally

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter MLD view.	**mld**	—
3. Configure the interface to discard any MLD message without the Router-Alert option.	**require-router-alert**	Optional. 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**	Optional. By default, MLD messages carry the Router-Alert option.

Configuring the Router-Alert option on an interface

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—

To do...	Use the command...	Remarks
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure the interface to discard any MLD message without the Router-Alert option.	**mld require-router-alert**	Optional. 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**	Optional. By default, MLD messages carry the Router-Alert option.

Configuring MLD query and response parameters

The MLD querier robustness variable defines the maximum number of attempts for transmitting MLD general queries, multicast-address-specific queries, or multicast-address-and-source-specific queries in the event of packet loss due to network issues. A larger robustness variable value makes the MLD querier "ore robust" but results in a longer IPv6 multicast group timeout.

On startup, the MLD querier sends **startup query count** MLD general queries at the **startup query interval**, which is 1/4 of the MLD query interval.

The MLD querier periodically sends MLD general queries at the MLD query interval to determine whether any IPv6 multicast group member exists on the network. You can modify the query interval based on the actual condition of the network.

Upon receiving an MLD done message, the MLD querier sends MLD multicast-address-specific queries (specifically, last listener query count) at the MLD last listener query interval. Upon receiving an MLD report concerning relation changes between IPv6 multicast groups and IPv6 multicast sources, the MLD querier sends a last listener query count MLD multicast-address-and-source-specific queries at the "MLD last listener query interval". The value of the "last listener query count" equals the value of the robustness variable.

Upon receiving an MLD query (general query, multicast-address-specific query, or multicast-address-and-source-specific query), a host starts a timer for each IPv6 multicast group that it has joined. The timer is initialized to a random value in the range of 0 to the maximum response delay. (the host obtains the maximum response delay from the Maximum Response Delay field in the MLD query message that it received). When the timer value drops to 0, the host sends an MLD membership report message to the corresponding IPv6 multicast group.

Proper setting of the maximum response delay of MLD query messages not only allows hosts to respond to MLD query messages quickly, but also avoids bursts of MLD traffic on the network. Such bursts can occur when a large number of hosts simultaneously send reports after corresponding timers expire.

- For MLD general queries, configure the maximum response delay to fill their Maximum Response Delay field.
- For MLD multicast-address-specific query and multicast-address-and-source-specific query messages, configure the last listener query interval to fill their Maximum Response Delay field (the maximum response time of MLD general query messages 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 within the other querier

present interval, it assumes that the querier has failed and a new querier election process begins. Otherwise, the non-querier resets the other querier present timer.

Configuring MLD query and response parameters globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter MLD view.	**mld**	—
3. Configure the MLD querier's robustness variable.	**robust-count** *robust-value*	Optional. 2 times by default.
4. Configure the startup query interval.	**startup-query-interval** *interval*	Optional. By default, the startup query interval is 1/4 of the "MLD query interval".
5. Configure the startup query count.	**startup-query-count** *value*	Optional. By default, the startup query count is set to the MLD querier's robustness variable.
6. Configure the MLD query interval.	**timer query** *interval*	Optional. 125 seconds by default.
7. Configure the maximum response delay for MLD general query messages.	**max-response-time** *interval*	Optional. 10 seconds by default.
8. Configure the MLD last listener query interval.	**last-listener-query-interval** *interval*	Optional. 1 second by default.
9. Configure the MLD other querier present interval.	**timer other-querier-present** *interval*	Optional. 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

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure the MLD querier's robustness variable.	**mld robust-count** *robust-value*	Optional. 2 times by default.

To do...	Use the command...	Remarks
4. Configure the startup query interval.	**mld startup-query-interval** *interval*	Optional. By default, the startup query interval is 1/4 of the "MLD query interval".
5. Configure the startup query count.	**mld startup-query-count** *value*	Optional. By default, the startup query count is set to the MLD querier's robustness variable.
6. Configure the MLD query interval.	**mld timer query** *interval*	Optional. Defaults to 125 seconds.
7. Configure the maximum response delay for MLD general query messages.	**mld max-response-time** *interval*	Optional. Defaults to 10 seconds.
8. Configure the MLD last listener query interval.	**mld last-listener-query-interval** *interval*	Optional. Defaults to 1 second.
9. Configure the MLD other querier present interval.	**mld timer other-querier-present** *interval*	Optional. 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.

Make sure that the other querier present interval is greater than the MLD query interval; otherwise the MLD querier may frequently change.

Make sure that the MLD query interval is greater than the maximum response delay for MLD general queries; otherwise, multicast group members may be wrongly removed.

Configuring MLD fast leave processing

MLD fast leave processing is implemented by MLD snooping. For more information about MLD snooping, see the chapter "MLD snooping configuration."

Configuring MLD SSM mapping

Because of possible restrictions, some receiver hosts on an SSM network might run MLDv1. To provide SSM service support for these receiver hosts, you must configure the MLD SSM mapping feature on the last hop router.

Prerequisites

Before configuring the MLD SSM mapping feature, complete the following tasks:

- Configure any IPv6 unicast routing protocol so that all devices in the domain can be interoperable at the network layer

- Configure MLD basic functions

Enabling MLD SSM mapping

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Enable the MLD SSM mapping feature.	**mld ssm-mapping enable**	Required. Defaults to disabled.

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

You can map an IPv6 multicast group to different IPv6 multicast sources by configuring this task repeately.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter MLD view.	**mld**	—
3. Configure an MLD SSM mapping.	**ssm-mapping** *ipv6-group-address prefix-length ipv6-source-address*	Required. No MLD mappings are configured by default.

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 configuring simulated joining with **mld-snooping host-join**.

In this case, the corresponding IPv6 multicast group will not be created based on the configured MLD SSM mappings. For more information about **mld-snooping host-join**, see *IP Multicast Command Reference*.

Configuring MLD proxying

Prerequisites

Before configuring the MLD proxying feature, complete the following tasks:

- Configure any 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.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Enable the MLD proxying feature.	**mld proxying enable**	Required. Defaults to disabled.

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 **mld require-router-alert**, **mld send-router-alert**, and **mld version** 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, **source-lifetime**, **source-policy** and **ssm-policy** 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.

Configuring IPv6 multicast forwarding on a downstream interface

Only queriers are able to forward IPv6 multicast traffic but non-queriers have no forwarding capabilities, to avoid duplicate multicast flows. It is the same on MLD proxy devices. Only the downstream interfaces acting as a querier can forward IPv6 multicast traffic to downstream hosts.

However, when a downstream interface of a proxy device fails to win the querier election, you need to enable IPv6 multicast forwarding on this interface.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Enable IPv6 multicast forwarding on a non-querier downstream interface.	**mld proxying forwarding**	Required. Defaults to disabled.

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 can be received on the multi-access network.

Displaying and maintaining MLD configuration

To do...	Use the command...	Remarks
Display MLD group information.	**display mld group** [*ipv6-group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display Layer 2 port information about MLD groups.	**display mld group port-info** [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

To do…	Use the command…	Remarks
Display MLD configuration and running information on the specified interface or all MLD-enabled interfaces.	**display mld interface** [*interface-type interface-number*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the information of the MLD proxying groups.	**display mld proxying group** [*group-address*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the information of the MLD routing table.	**display mld routing-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **flags** { **act** | **suc** }] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display MLD SSM mappings.	**display mld ssm-mapping** *ipv6-group-address* [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the IPv6 multicast group information created based on the configured MLD SSM mappings.	**display mld ssm-mapping group** [*ipv6-group-address* | **interface** *interface-type interface-number*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Remove the dynamic group entries of a specified MLD group or all MLD groups.	**reset mld group** { **all** | **interface** *interface-type interface-number* { **all** | *ipv6-group-address* [*prefix-length*] [*ipv6-source-address* [*prefix-length*]] } }	Available in user view
Remove the dynamic Layer 2 port entries of a specified MLD group or all MLD groups.	**reset mld group port-info** { **all** | *ipv6-group-address* } [**vlan** *vlan-id*]	Available in user view
Clear MLD SSM mappings.	**reset mld ssm-mapping group** { **all** | **interface** *interface-type interface-number* { **all** | *ipv6-group-address* [*prefix-length*] [*ipv6-source-address* [*prefix-length*]] } }	Available in user view

The **reset mld group** command cannot remove dynamic MLD group entries.

The **reset mld group port-info** command cannot remove the Layer 2 port entries of MLD groups.

The **reset mld group** command can cause an interruption of receivers' reception of multicast data.

MLD configuration examples

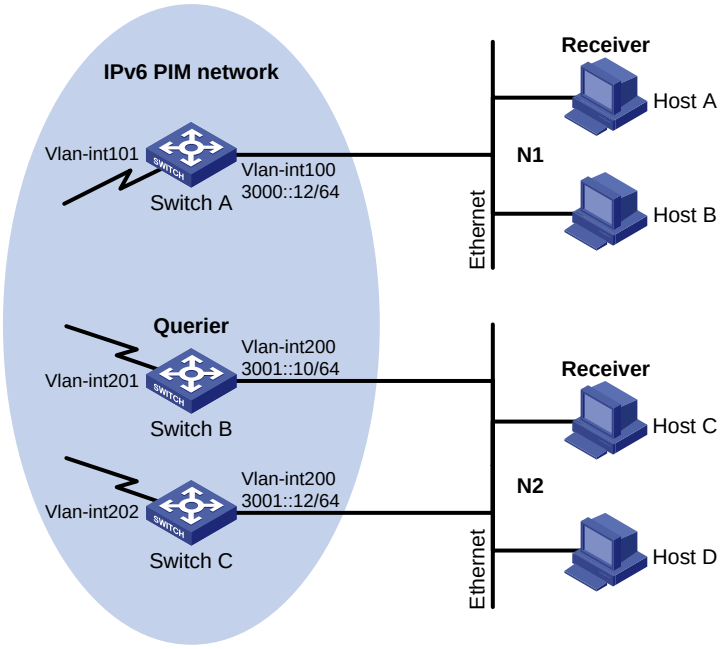
Basic MLD functions configuration example

Network requirements

- As shown in Figure 96, 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.
- Switch A in the IPv6 PIM network connects to N1, and Switch B and Switch C connect to N2.
- Switch A connects to N1 through VLAN-interface 100, and to other devices in the IPv6 PIM network through VLAN-interface 101.
- Switch B and Switch C connects to N2 through their own VLAN-interface 200, and to other devices in the IPv6 PIM network through VLAN-interface 201 and VLAN-interface 202 respectively.

- MLDv1 is required between Switch A and N1. MLDv1 is also required 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.

Figure 96 Network diagram for basic MLD functions configuration



Procedure

1. Enable IPv6 forwarding and configure IPv6 addresses and IPv6 unicast routing

Enable IPv6 forwarding on each switch and configure an IP address and prefix length for each interface as shown in Figure 96. The detailed configuration steps are not discussed in this document.

Configure OSPFv3 for interoperation between the switches. Ensure the network-layer interoperation among the switches on the IPv6 PIM network and dynamic update of routing information between the switches through a unicast routing protocol. The detailed configuration steps are omitted here.

2. Enable the IPv6 multicast routing, and enable IPv6 PIM-DM and MLD.

Enable IPv6 multicast routing on Switch A, enable IPv6 PIM-DM on each interface, and enable MLD on VLAN-interface 100.

```
<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 IPv6 PIM-DM on each interface, and enable MLD on VLAN-interface 200.

```
<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
```

3. Verify the configuration

Carry out the **display mld interface** command to display the MLD configuration and running information on each switch interface. Example:

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

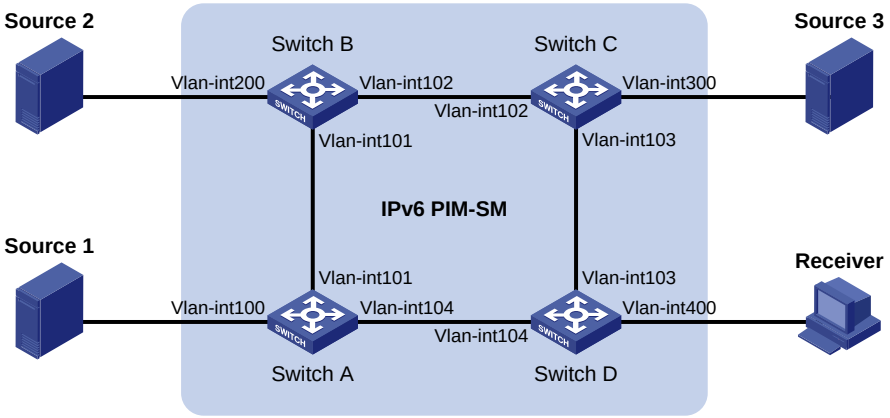
```
[SwitchB] display mld interface vlan-interface 200
 Vlan-interface200(FE80::200:5EFF:FE66:5100):
   MLD is enabled
   Current MLD version is 1
   Value of query interval for MLD(in seconds): 125
   Value of other querier present interval for MLD(in seconds): 255
   Value of maximum query response 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 97, 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. Be sure to 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 97 Network diagram for MLD SSM mapping configuration



Device	Interface	IP address	Device	Interface	IP 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

Procedure

1. Enable IPv6 forwarding and configure IPv6 addresses and IPv6 unicast routing

Enable IPv6 forwarding on each switch and configure an IPv6 address and prefix length for each interface as shown in Figure 97. The detailed configuration steps are omitted.

Configure OSPFv3 for interoperability among the switches. Ensure the network-layer interoperation on the IPv6 PIM-SM domain and dynamic update of routing information among the switches through an IPv6 unicast routing protocol. The detailed configuration steps are omitted here.

2. 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 MLDv2 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
```

The configuration on Switch B and Switch C is similar to that on Switch A.

3. Configure a C-BSR and a C-RP

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
```

4. 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
```

The configuration on Switch A, Switch B and Switch C is similar to that on Switch D.

5. Configure MLD SSM mappings

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
```

6. Verify the configuration

Use **display mld ssm-mapping** to view MLD SSM mappings on the switch.

Display the MLD SSM mapping information for IPv6 multicast group FF3E::101 on Switch D.

```
[SwitchD] display mld ssm-mapping ff3e::101
Group: FF3E::101
Source list:
```

```
       1001::1
       3001::1
```

Use **display mld ssm-mapping group** to view information of the MLD groups created based on the configured MLD SSM mappings.

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
```

Use **display pim ipv6 routing-table** to view the IPv6 PIM routing table information on each switch.

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: -
```

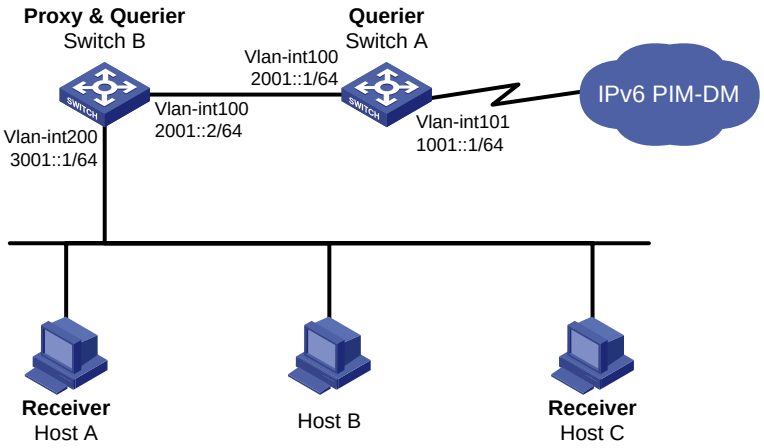
MLD proxying configuration example

Network requirements

As shown in Figure 98, IPv6 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 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 98 Network diagram for MLD proxying configuration



Procedure

1. Enable IPv6 forwarding and configure the IPv6 addresses

Enable IPv6 forwarding on each switch and configure the IPv6 address and prefix length of each interface as shown in Figure 98. The detailed configuration steps are omitted here.

2. Enable IPv6 multicast routing, IPv6 PIM-DM, MLD, and MLD proxying respectively.

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
```

3. Verify the installation

Use the **display mld interface** command to view the MLD configuration and operation information on an interface. For example,

Display MLD configuration and operation 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
```

Use the **display mld group** command to view MLD group information. For example,

Display the 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 for 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. Verify that the networking, interface connections, and IP address configuration are correct. Evaluate the interface information by using 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. Verify that the IPv6 multicast routing is enabled. Use the **display current-configuration** command to check whether the **multicast ipv6 routing-enable** command has been executed. If not, use the **multicast ipv6 routing-enable** command in system view to enable IPv6 multicast routing. In addition, enable MLD on the corresponding interface.
3. Verify the MLD version on the interface. Use the **display mld interface** command to determine whether the MLD version on the interface is lower than that on the host.
4. Verify that no ACL rule has been configured to restrict the host from joining IPv6 multicast group G. Use the **display current-configuration interface** command to determine whether the **mld group-policy** command has been executed. 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 that is 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 cause inconsistent MLD memberships.
- Two MLD versions are currently available. Although routers that are running different MLD versions are compatible with hosts, all routers on the same subnet must run the same MLD version. Inconsistent MLD versions that are running on routers on the same subnet will also lead to inconsistent MLD memberships.

Solution

1. Evaluate MLD configurations. Use the **display current-configuration** command to display the MLD configuration information on the interface.
2. Use **display mld interface** on all routers on the same subnet to check the MLD timers for consistent configurations.
3. Use **display mld interface** to verify that the routers are running the same MLD version.

Configuring IPv6 PIM

IPv6 PIM provides IPv6 multicast forwarding by leveraging 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 RPF verification to implement IPv6 multicast forwarding.

Independent of the IPv6 unicast routing protocols that are running on the switch, you can implement IPv6 multicast routing as long as you create the corresponding IPv6 multicast routing entries through IPv6 unicast routes. IPv6 PIM uses the RPF mechanism to implement IPv6 multicast forwarding. When an IPv6 multicast packet arrives on a switch interface, it undergoes an RPF verification. If the RPF verification succeeds, the switch creates the corresponding routing entry and forwards the packet. If the RPF verification fails, the switch discards the packet. For more information about RPF, see the chapter "IPv6 multicast routing and forwarding configuration."

Based on the implementation mechanism, IPv6 PIM falls into the following modes:

- IPv6 PIM-DM
- IPv6 PIM-SM

Interface view mentioned in this chapter can be VLAN interface view or Layer 3 Ethernet interface view. Layer 3 Ethernet interfaces refer to Ethernet interfaces configured to operate in route mode. To switch the operating mode of an Ethernet port, see *Layer 2 - LAN Switching Configuration Guide*.

To facilitate description, a network comprising IPv6 PIM–supporting routers is referred to as an "IPv6 PIM domain" in this document.

Understanding IPv6 PIM-DM

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, and 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. 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, namely, 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 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.

Every IPv6 PIM enabled interface on a router sends hello messages periodically, and thus learns the IPv6 PIM neighboring information pertinent to the interface.

SPT establishment

The process of constructing an SPT is the flood-and-prune process.

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 is subject to an RPF verification. If the packet passes the RPF verification, 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.

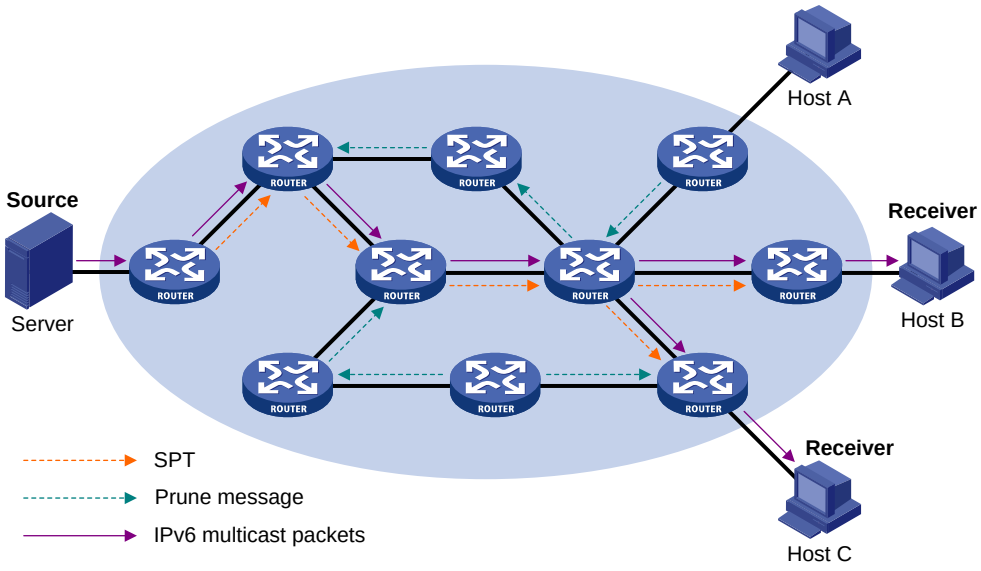
Nodes without downstream receivers are pruned. A router that has no downstream receivers sends a prune message to the upstream node to notify the upstream node to delete the corresponding interface from the outgoing interface list in the (S, G) entry and stop forwarding subsequent packets addressed to 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 99, 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 99 SPT establishment in an IPv6 PIM-DM domain



The flood-and-prune process occurs periodically. A pruned state timeout mechanism exists. 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.

Pruning has a similar implementation in IPv6 PIM-SM.

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:

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.

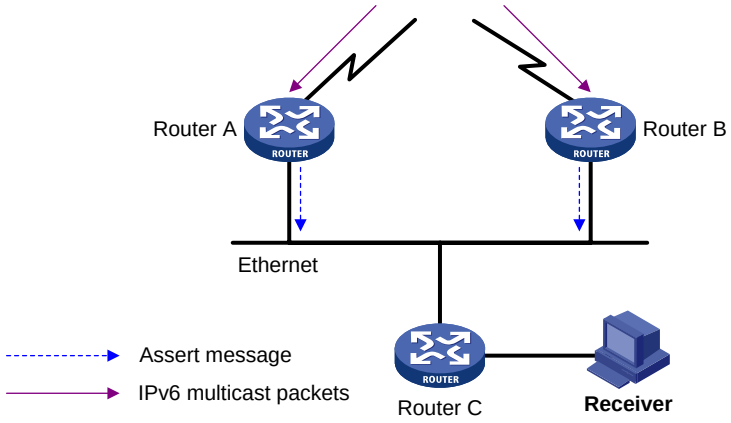
Upon receiving this graft message, the upstream node puts the interface on which the graft was received into the forwarding state and responds with a graft-ack message to the graft sender.

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

The assert mechanism shuts off duplicate IPv6 multicast flows onto the same multi-access network, where more than one multicast routers exists, by electing a unique IPv6 multicast forwarder on the multi-access network.

Figure 100 Assert mechanism



As shown in Figure 100, 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 local interface, receive a duplicate IPv6 multicast packet that the other has forwarded.

Upon detecting this condition, both routers send an assert message to all IPv6 PIM routers on the local subnet through the 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 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:

- The router with a higher IPv6 unicast route preference to the source wins.
  - If both routers have the same IPv6 unicast route preference to the source, the router with a smaller metric to the source wins.
  - If a tie in the route metric to the source exists, the router with a higher IPv6 link-local address wins.

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 PIM-DM mode is not suitable for large-sized and medium-sized networks.

Understanding IPv6 PIM-SM

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 builds and maintains RPTs. An RPT is rooted at a router in the IPv6 PIM domain as the common node, or RP, through which the IPv6 multicast data travels along the RPT and reaches the receivers.
- When a receiver is available for the IPv6 multicast data addressed to a specific IPv6 multicast group, the router connected to this receiver sends a join message to the RP that corresponds 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 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 IPv6 multicast source sends subsequent IPv6 multicast packets along the SPT to the RP. Upon reaching the RP, the IPv6 multicast packet is duplicated and delivered to the receivers along the RPT.

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 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.

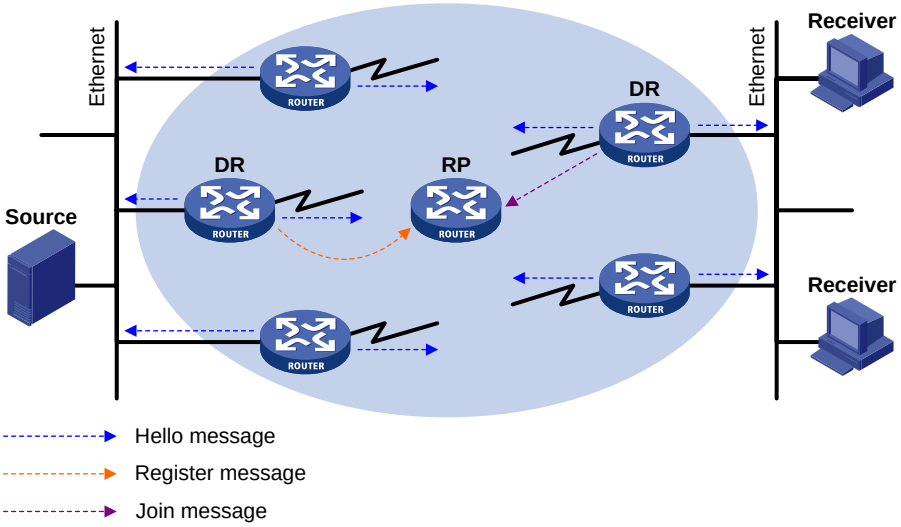
In the case of a multi-access network, a DR must be elected, whether this network connects to IPv6 multicast sources or to receivers. The DR at the receiver side sends join messages to the RP. The DR at the IPv6 multicast source side sends register messages to the RP.

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 *IP Multicast Configuration Guide*.

Figure 101 DR election



As shown in Figure 101, the DR election process is as follows:

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.

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, and 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.

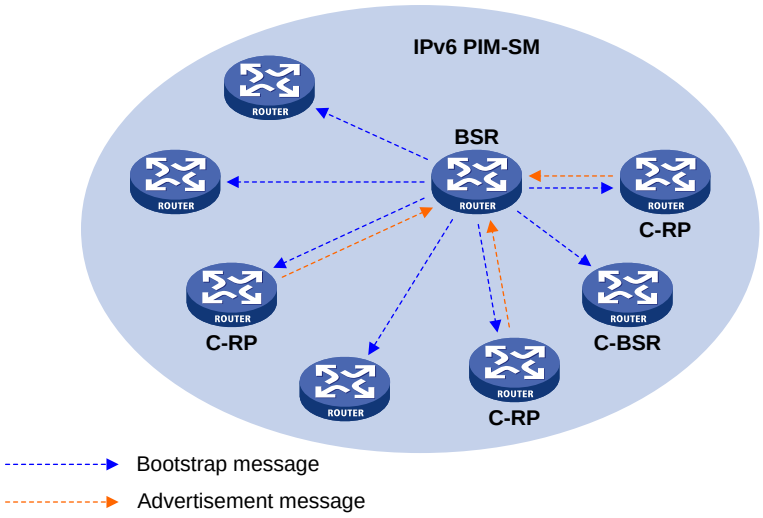
To lessen the RP burden and optimize the topological structure of the RPT, you can configure C-RPs in an IPv6 PIM-SM domain. Among them, an RP is dynamically elected through the bootstrap mechanism. Each elected RP serves a different multicast group range. For this purpose, you must configure a BSR. The BSR serves 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.

An RP can serve IPv6 multiple multicast groups or all IPv6 multicast groups. Only one RP can serve a given IPv6 multicast group at a time.

A device can server as a C-RP and a C-BSR at the same time.

As shown in Figure 102, each C-RP periodically unicasts its advertisement messages (C-RP-Adv messages) to the BSR. A C-RP-Adv message contains the address of the advertising C-RP and the IPv6 multicast group range it serves. The BSR collects these advertisement messages and chooses the appropriate C-RP information for each multicast group to form 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 it periodically originates and floods the bootstrap messages (BSMs) to the entire IPv6 PIM-SM domain.

Figure 102 BSR and C-RPs



Based on the information in the RP-sets, all routers in the network can calculate the location of the corresponding RPs based on the following rules:

1. The C-RP with the highest priority wins.
2. If all the C-RPs have the same priority, their hash values are calculated through the hashing algorithm. The C-RP with the largest hash value wins.
3. If all the C-RPs have the same priority and hash value, the C-RP with 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 2^{31}.

Table 17 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 XOR 0x01A30063 XOR 0x00000000 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 XOR 0x0C180001 XOR 0x00000000 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 know the RP address beforehand. The specific process is as follows.

At the receiver side, the following process occurs:

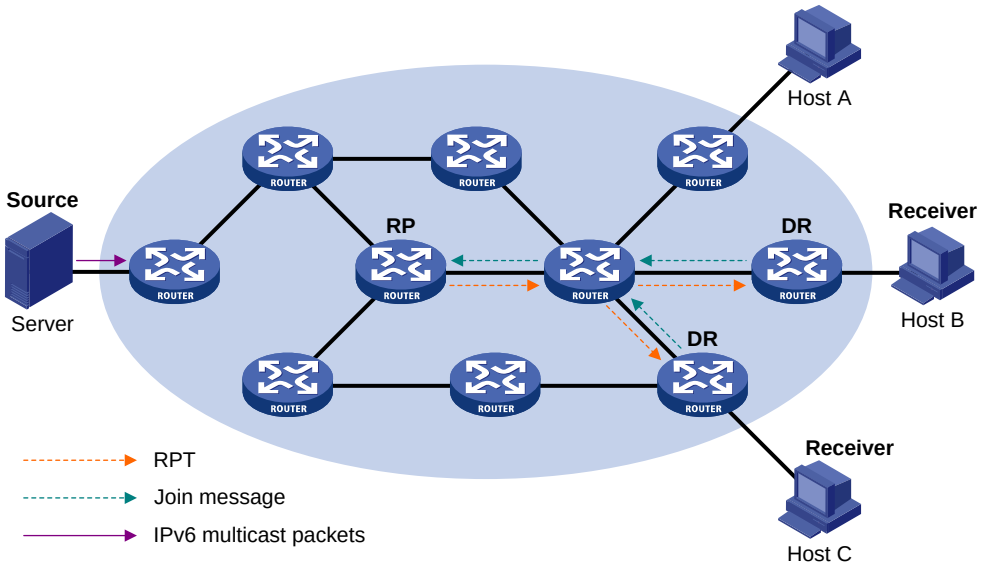
1. A receiver host initiates an MLD report to announce its joining an IPv6 multicast group.
2. Upon receiving the MLD report, the receiver-side DR resolves the RP address embedded in the IPv6 multicast address, and sends a join message to the RP.

At the IPv6 multicast source side, the following process occurs:

3. The IPv6 multicast source sends IPv6 multicast traffic to the IPv6 multicast group.
4. 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 103 RPT establishment in an IPv6 PIM-SM domain



As shown in Figure 103, 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. Upon 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, and the DRs are the leaves, of the RPT.

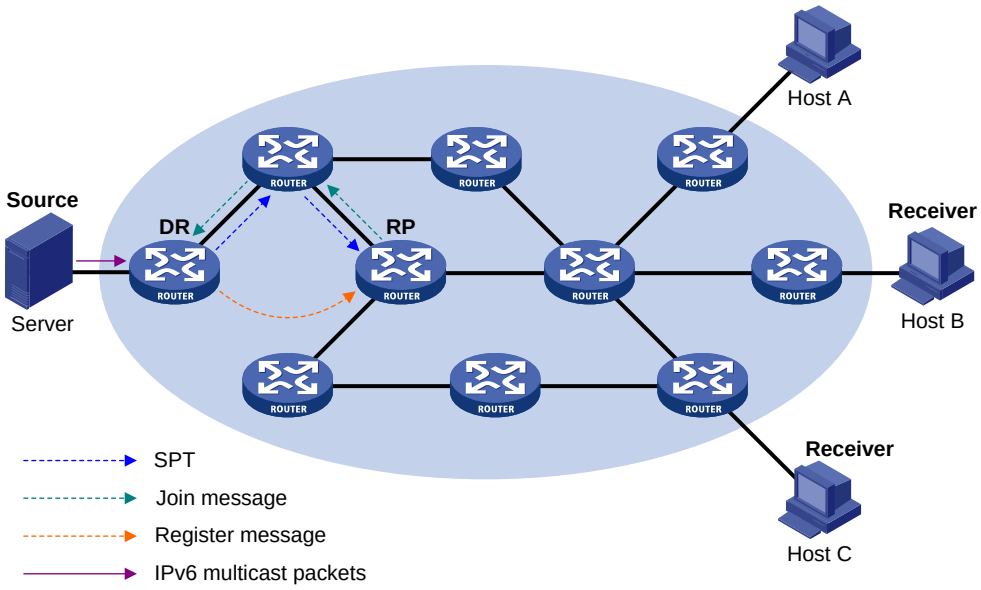
The IPv6 multicast data addressed to the IPv6 multicast group G flows through the RP, reaches the corresponding DR along the established RPT, and finally is delivered to the receiver.

When a receiver is no longer available for 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. Upon 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 is to inform the RP about the existence of the IPv6 multicast source.

Figure 104 IPv6 multicast source registration



As shown in Figure 104, the IPv6 multicast source registers with the RP as follows:

1. When the IPv6 multicast source S sends the first IPv6 multicast packet to IPv6 multicast group G, the DR directly connected with the multicast source, upon receiving the multicast packet, encapsulates the packet in a register message, and 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. Thus, 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, 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.

The RP is configured to initiate an SPT switchover 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 SPT switchover 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. Upon 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 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 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 an SPT switchover process when the traffic rate exceeds the threshold.

The RP initiates an SPT switchover process.

Upon receiving the first IPv6 multicast packet, the RP will 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 SPT switchover initiated by the RP, see "Multicast source registration."

The receiver-side DR initiates an SPT switchover process

Upon 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 created 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. Upon receiving this prune message, the RP sends a prune message toward the IPv6 multicast source (suppose only one receiver exists), in order to implement the SPT switchover.
- Finally, 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 the similar assert mechanism as IPv6 PIM-DM does.

Understanding IPv6 BIDIR-PIM

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.

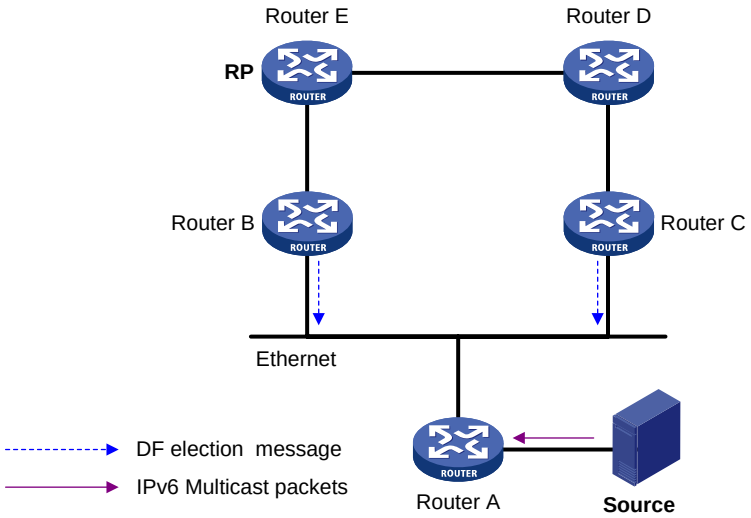
In IPv6 BIDIR-PIM, an RPF interface is the interface pointing to an RP, and an RPF neighbor is the address of the next hop to the RP.

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.

DF election is not necessary for an RPL.

Figure 105 DF election



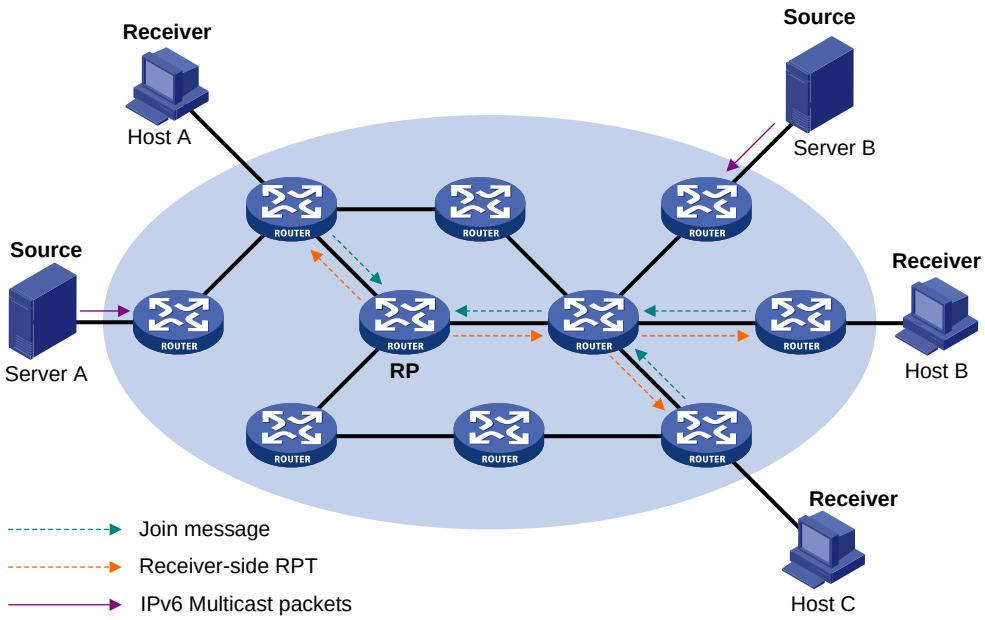
As shown in Figure 105, without the DF election mechanism, both Router B and Router C can receive multicast packets from Route A, and they might both forward the packets to downstream routers on the local subnet. As a result, the RP—Router E—receives duplicate multicast packets. With the DF election 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 multicast static 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 receiver-side RPT and 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 106 RPT building at the receiver side

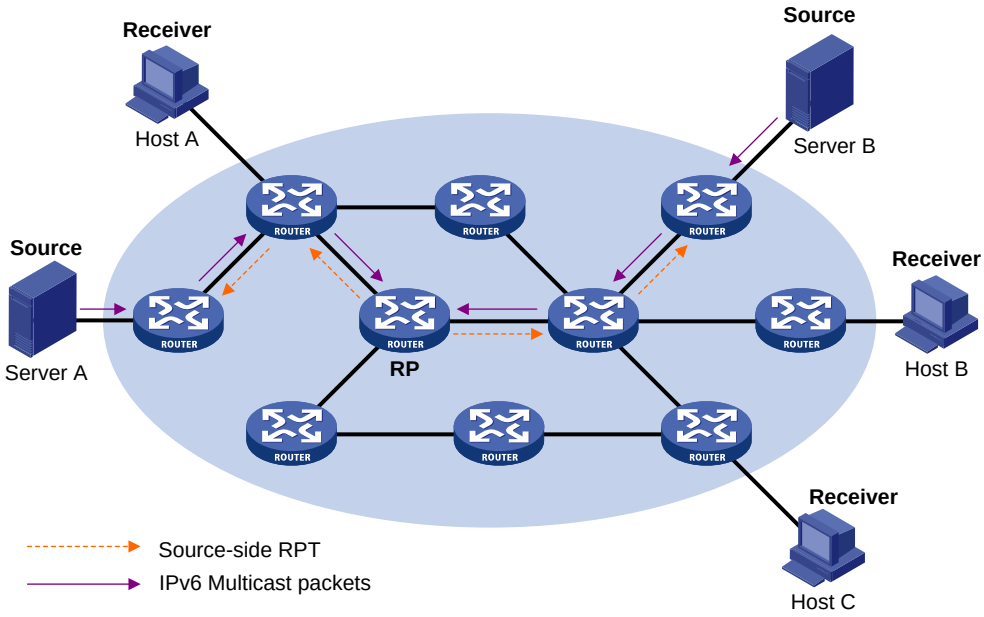


As shown in Figure 106, the process for building a receiver-side RPT is similar to that for building an RPT in IPv6 PIM-SM:

1. When a receiver joins IPv6 multicast group G, it uses an IGMP message to inform the directly connected router.
2. Upon 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. Upon 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 107 RPT building at the multicast source side



As shown in Figure 107, the process of building a source-side RPT is relatively simple:

4. 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.
5. 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.

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 are directly forwarded by the node to the receiver, instead of by the RP.

IPv6 administrative scoping

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. This is called "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). This is called "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 serves 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 served by different IPv6

admin-scope zones 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 serves the IPv6 multicast groups with the Scope field in their group addresses being 14.

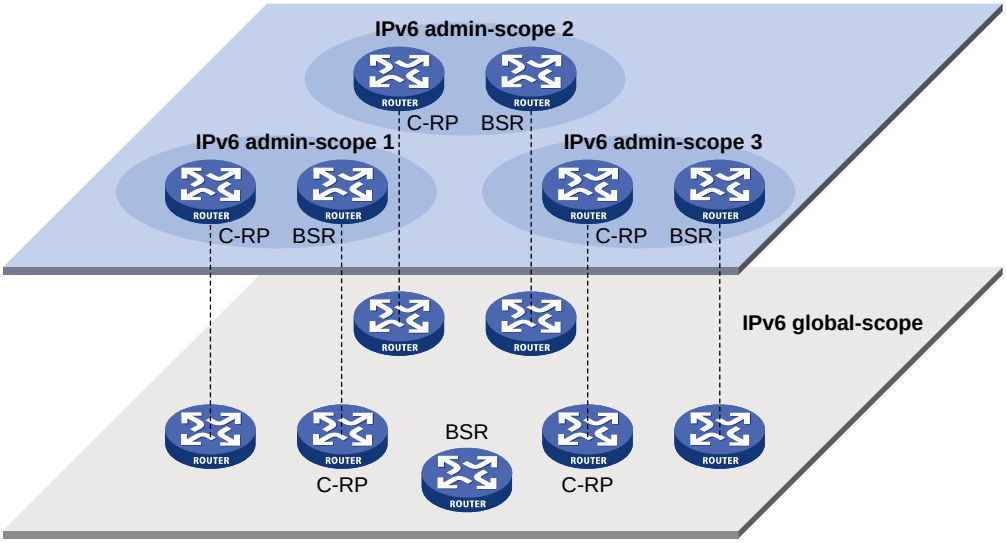
IPv6 admin-scope zones and the IPv6 global scope zone

The IPv6 global scope zone and each IPv6 admin-scope zone have their own C-RPs and BSRs. These devices are effective only in their respective IPv6 admin-scope zones. Namely, BSR election and RP election are implemented independently within each IPv6 admin-scope zone. Each IPv6 admin-scope zone has its own boundary. The multicast information cannot cross this border in either direction. A better understanding of the IPv6 global scope zone and IPv6 admin-scope zones should be based on geographical space and group address range.

Geographical space

IPv6 admin-scope zones are logical zones specific to particular multicast groups. The multicast packets of these multicast groups are confined within the local IPv6 admin-scope zone and cannot cross the boundary of the zone.

Figure 108 Relationship between admin-scope zones and the global scope zone in geographic space

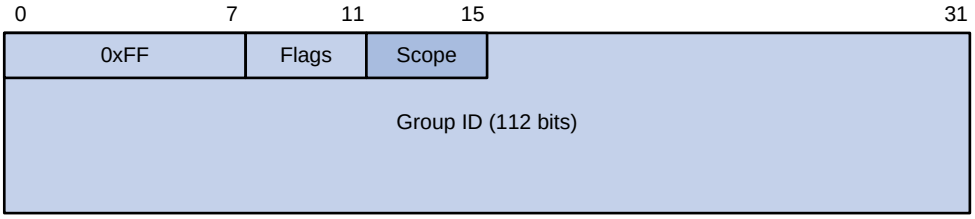


As shown in Figure 108, for multicast groups with the same Scope field in their group addresses, IPv6 admin-scope zones must be geographically separated from one another. Namely, a router must not serve different admin-scope zones. In other words, different admin-scope zones contain different routers, whereas the global scope zone covers all routers in the IPv6 PIM-SM/IPv6 BIDIR-PIM domain. Multicast packets that do not belong to any admin-scope zones can be transmitted in the entire IPv6 PIM-SM/IPv6 BIDIR-PIM domain.

In terms of multicast group address Scope field

As shown in Figure 109, the Scope field in each IPv6 multicast group address indicates the admin-scope zone the corresponding multicast group belongs to.

Figure 109 IPv6 multicast address format



The admin-scope zone range increases with the value of the Scope field. For example, value E indicates IPv6 global scope, which contains other admin-scope zones with the Scope field values smaller than E.

Table 18 Values of the Scope field

Value	Meaning	Remarks
0, F	Reserved	—
1	Interface-local scope	—
2	Link-local scope	—
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

Implementing an SSM model in IPv6 PIM

The SSM model and the 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.

The SSM model provides a solution for source-specific multicast. It maintains the relationships between hosts and routers through MLDv2. IPv6 PIM-DM implements IPv6 multicast forwarding by building SPTs rooted at the IPv6 multicast source through the flood-and-prune mechanism. Although an SPT has the shortest path, it is built in a low efficiency. Therefore, the IPv6 PIM-DM mode is not suitable for large-sized and medium-sized networks.

In actual application, you adopt part of the IPv6 PIM-SM technique to implement the SSM model. In the SSM model, receivers locate an IPv6 multicast source 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.

The operation mechanism of the IPv6 PIM-SSM can be 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.

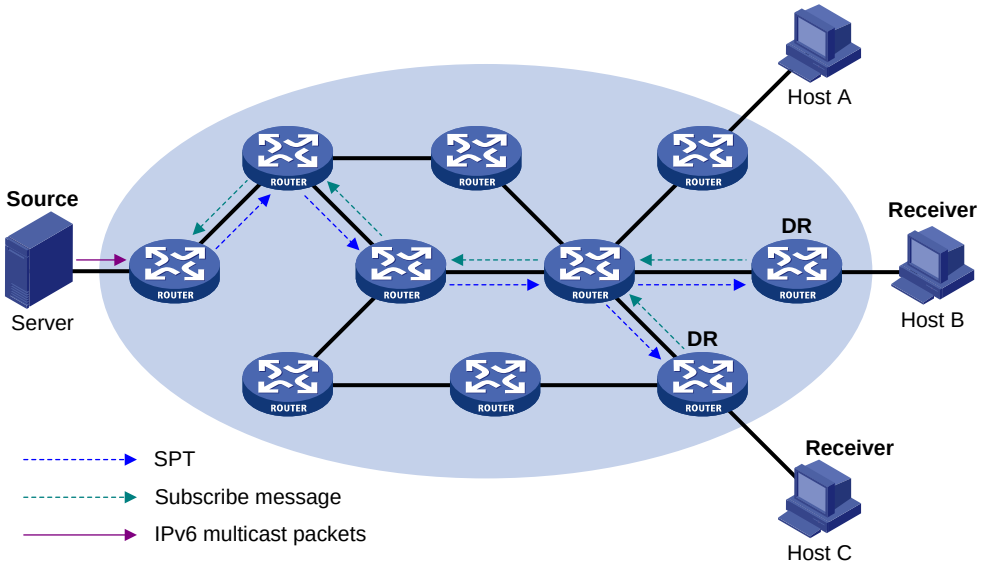
DR election

IPv6 PIM-SSM uses the same DR election mechanism as in IPv6 PIM-SM. For more information, see "DR election."

SPT building

Whether 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 in the IPv6 SSM group range. (The IPv6 SSM group range reserved by IANA is FF3x::/32, where x represents any legal address scope).

Figure 110 Building an SPT in IPv6 PIM-SSM



As shown in Figure 110, Hosts B and C are IPv6 multicast information receivers. They send an MLDv2 report message to the respective DRs to announce that they are available for 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 in the IPv6 SSM group range.

- If so, 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 not, the IPv6 PIM-SM process occurs. The DR must send a (*, G) join message to the RP, and an IPv6 multicast source registration process is needed.

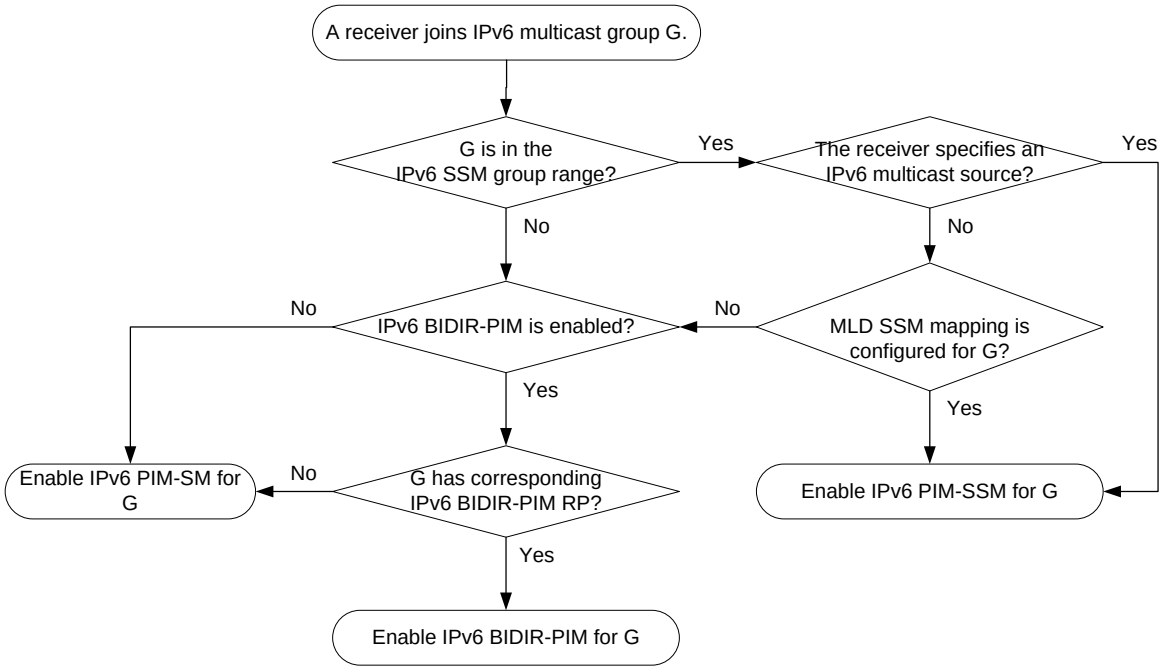
In IPv6 PIM-SSM, the term *channel* refers to an IPv6 multicast group, and the term *channel subscription* refers to a join message.

Understanding IPv6 PIM protocol relationships

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,

they are adopted in the order of IPv6 PIM-SSM, IPv6 BIDIR-PIM, and IPv6 PIM-SM, as shown in Figure 111. For more information about MLD SSM mapping, see "Configuring MLD."

Figure 111 Selection of IPv6 PIM-SM, IPv6 BIDIR-PIM, and IPv6 PIM-SSM



Protocols and standards

IPv6 PIM–related specifications are as follows:

- 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

Prerequisites

Before configuring IPv6 PIM-DM, complete the following tasks:

- Enable IPv6 forwarding and configure any 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.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enable IPv6 multicast routing.	**multicast ipv6 routing-enable**	Required. Disable by default.
3. Enter interface view.	**interface** *interface-type interface-number*	—
4. Enable IPv6 PIM-DM.	**pim ipv6 dm**	Required. Defaults to disabled.

All the interfaces of the same device must work in the same IPv6 PIM mode.

IPv6 PIM-DM cannot be used for IPv6 multicast groups in the IPv6 SSM group range.

For more information about **multicast ipv6 routing-enable**, 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 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
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 an interval for sending such messages.

A router can receive multiple state-refresh messages within a short time and some might be duplicate 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, the router will discard 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.

To configure state-refresh parameters, complete the following steps. HP recommends that you perform the configuration on all routers in the IPv6 PIM domain.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure the interval between state-refresh messages.	**state-refresh-interval** *interval*	Optional. Defaults to 60 seconds.
4. Configure the time to wait before receiving a new state-refresh message.	**state-refresh-rate-limit** *interval*	Optional. Defaults to 30 seconds.
5. Configure the hop limit value of state-refresh messages.	**state-refresh-hoplimit** *hoplimit-value*	Optional. Defaults to 255.

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, the graft retry period—until it receives a graft-ack message from the upstream router.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure graft retry period.	**pim ipv6 timer graft-retry** *interval*	Optional. 3 seconds by default.

Configuring IPv6 PIM-SM

Prerequisites

Before configuring IPv6 PIM-SM, complete the following tasks:

- Enable IPv6 forwarding and configure any 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 IPv6 ACL that defines the range of IPv6 multicast groups that the static RP will serve
- Determine the C-RP priority and the IPv6 ACL that defines the range of IPv6 multicast groups to be served by each C-RP
- Determine the legal C-RP address range and the IPv6 ACL that define the range of IPv6 multicast groups to be served

- 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 for register message filtering
- Determine the register suppression time
- Determine the register probe time
- Determine the IPv6 ACL, and sequencing rule for disabling 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.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enable IPv6 multicast routing.	**multicast ipv6 routing-enable**	Required. Disable by default
3. Enter interface view.	**interface** *interface-type interface-number*	—
4. Enable IPv6 PIM-SM.	**pim ipv6 sm**	Required. Defaults to disabled.

All the interfaces of the same device must work in the same IPv6 PIM mode.

For more information about **multicast ipv6 routing-enable**, see *IP Multicast Command Reference*.

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.

Configuring a static RP

If only one dynamic RP exists in a network, configuring a static RP can avoid communication interruption due to single-point failures and avoid frequent message exchange between C-RPs and the BSR.

Perform the following configuration on all the routers in the IPv6 PIM-SM domain.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—

To do...	Use the command...	Remarks
3. Configure a static RP for IPv6 PIM-SM.	**static-rp** *ipv6-rp-address* [*acl6-number*] [**preferred**]	Required. No static RP by default.

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.

Configuring a C-RP

In an IPv6 PIM-SM domain, you can configure routers that will 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 must configure a legal C-RP address range and the range of IPv6 multicast groups to be served on the BSR. In addition, because every C-BSR can become the BSR, be sure to configure the same filtering policy on all C-BSRs in the IPv6 PIM-SM domain.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure an interface to be a C-RP for IPv6 PIM-SM.	**c-rp** *ipv6-address* [{ **group-policy** *acl6-number* | **scope** *scope-id* } | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] *	Required. No C-RPs are configured by default.
4. Configure a legal C-RP address range and the range of IPv6 multicast groups to be served.	**crp-policy** *acl6-number*	Optional. No restrictions by default.

When configuring a C-RP, ensure a relatively large bandwidth between this C-RP and the other devices in the IPv6 PIM-SM domain.

An RP can serve multiple IPv6 multicast groups or all IPv6 multicast groups. Only one RP can forward IPv6 multicast traffic for an IPv6 multicast group at a moment.

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.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—

To do...	Use the command...	Remarks
3. Enable embedded RP.	**embedded-rp** [*acl6-number*]	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* in the *IP Multicast Configuration Guide*.

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. Upon receiving a C-RP-Adv message, the BSR obtains this timeout value and starts a C-RP timeout timer. If the BSR fails to find 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 must be configured on C-RP routers.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure the C-RP-Adv interval.	**c-rp advertisement-interval** *interval*	Optional. Defaults to 60 seconds.
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 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

HP recommends that you configure C-BSRs on routers in the backbone network. When you are configuring 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 summarized 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

in the priority exists, 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, but the winner keeps 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, in order to prevent a maliciously configured host from masquerading as a BSR. You must make the same configuration on all routers in the IPv6 PIM-SM domain. The following are typical BSR spoofing cases and the corresponding preventive measures:

1. 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 verifications and RPF verifications on bootstrap messages and discard unwanted messages.
2. When an attacker controls a router in the network or when 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 it is 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 previously mentioned preventive measures can partially protect the security of BSRs in a network. However, the issue also occurs if an attacker controls a legal BSR.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure an interface as a C-BSR.	**c-bsr** *ipv6-address* [*hash-length* [*priority*]]	Required. No C-BSRs are configured by default.
4. Configure a legal BSR address range.	**bsr-policy** *acl6-number*	Optional. No restrictions by default.

Since 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.

Configuring an IPv6 PIM domain border

In each IPv6 PIM-SM domain, a unique BSR is elected from C-BSRs. The C-RPs in the IPv6 PIM-SM domain administrative core send advertisement messages tothe BSR. The BSR summarizes the advertisement messages to form an RP-set and advertises 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. A number of IPv6 PIM domain border interfaces partition a network into different IPv6 PIM-SM domains. Bootstrap messages cannot cross a domain border in either direction.

Use the following configuration procedure on routers that can become an IPv6 PIM domain border.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—

To do...	Use the command...	Remarks
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configuring an IPv6 PIM domain border.	**pim ipv6 bsr-boundary**	Required. No IPv6 PIM domain border is configured by default

Configuring C-BSR parameters globally

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 corresponding to specific IPv6 multicast groups.

Perform the following configuration on C-BSR routers.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure the hash mask length.	**c-bsr hash-length** *hash-length*	Optional. 126 by default.
4. Configure the C-BSR priority.	**c-bsr priority** *priority*	Optional. 64 by default.

Configuring C-BSR timers

The BSR election winner multicasts its own IPv6 address and RP-set information throughout the region that it serves through bootstrap messages. The BSR floods bootstrap messages throughout the network at the interval of the BS (BSR state). 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 the BSR state times out and no bootstrap message is received from the BSR, a new BSR election process begins among the C-BSRs.

Perform the following configuration on C-BSR routers. Make sure that the BS period is smaller than the BS timeout value.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure the BS period.	**c-bsr interval** *interval*	Optional. For the default value, see the note under this table.
4. Configure the BS timeout.	**c-bsr holdtime** *interval*	Optional. For the default value, see the note under this table.

BS period and timeout settings

Make sure that the BS period value is smaller than the BS timeout value.

The BS period defaults to the value 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 timeout setting defaults to the value determined by the formula:

"BS timeout = BS period × 2 + 10". The default BS period is 60 seconds, so the default BS timeout = 60 × 2 + 10 = 130 (seconds)

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).

- Upon 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 upon 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.

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 PIM-SM domain, you need to disable the semantic fragmentation function on the C-BSRs.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Disable the BSM semantic fragmentation function.	**undo bsm-fragment enable**	Required. By default, the BSM semantic fragmentation function is enabled.

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 IPv6 PIM neighbor is performed according to the MTU of the outgoing interface.

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, partition the IPv6 PIM-SM domain into multiple IPv6 admin-scope zones. Each IPv6 admin-scope zone maintains a BSR, which serves a specific IPv6 multicast group range, and the IPv6 global scope zone also maintains a BSR, which serves the IPv6 multicast groups with the Scope field in the group addresses being 14.

Enabling IPv6 administrative scoping

Before configuring an IPv6 admin-scope zone, you must enable IPv6 administrative scoping first. Use following configuration on routers that can become a C-BSR and ZBR.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Enable IPv6 administrative scoping.	**c-bsr admin-scope**	Required. Defaults to disabled.

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 serves 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.

Use the following configuration for routers that can become a ZBR.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure an IPv6 multicast forwarding boundary.	**multicast ipv6 boundary** { *ipv6-group-address prefix-length* | **scope** { *scope-id* | **admin-local** | **global** | **organization-local** | **site-local** } }	Required. By default, no multicast forwarding boundary is configured.

For more information about the **multicast ipv6 boundary** command, see *IP Multicast Command Reference*.

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. 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.

Perform the following configuration on the routers that will work as C-BSRs in IPv6 admin-scope zones.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure a C-BSR for an IPv6 admin-scope zone.	**c-bsr scope** { *scope-id* | **admin-local** | **global** | **organization-local** | **site-local** } [**hash-length** *hash-length* | **priority** *priority*] *	Required. No C-BSRs are configured for an IPv6 admin-scope zone by default.

Hash mask length and C-BSR priority

You can configure these parameters at three levels:

- Global configuration level
- Global scope zone level

- Admin-scope zone level

Parameter values configured at the global scope zone level or admin-scope zone level have preference over the global configuration level values, and default to the global value level.

For configuration of global C-BSR parameters, see "Configuring global C-BSR parameters."

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 serve 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 (that is, the RP stops serving the receivers of that IPv6 multicast group), or when the RP formally starts receiving register messages with IPv6 multicast data encapsulated from the IPv6 multicast source, the RP sends a register-stop message to the source-side DR. Upon receiving this message, the DR stops sending register messages encapsulated with IPv6 multicast data and starts a register-stop timer. When 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure a filtering rule for register messages.	**register-policy** *acl6-number*	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** *interval*	Optional. Defaults to 60 seconds.
6. Configure the register probe time.	**probe-interval** *interval*	Optional. Defaults to 5 seconds.

Disabling SPT switchover

In an A5820X or A5800 switch acts as an RP or the receiver-side DR, it initiates an STP switchover process by default upon receiving the first IPv6 multicast packet along the RPT. You can disable the switchover from RPT to SPT.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Disable the SPT switchover.	**spt-switch-threshold infinity** [**group-policy** *acl6-number* [**order** *order-value*]]	Optional. By default, the device switches to the SPT immediately after it receives the first IPv6 multicast packet from the RPT.

For an A5820X&A5800 Series Ethernet switch, once an IPv6 multicast forwarding entry is created, subsequent IPv6 multicast data will not be encapsulated in register messages before being forwarded even if a register outgoing interface is available. Therefore, to avoid forwarding failure, do not use **spt-switch-threshold infinity** on a switch that may become an RP (a static RP or a C-RP).

Configuring IPv6 PIM-SSM

The IPv6 PIM-SSM model needs the support of MLDv2. Be sure to configure IPv6 BIDIR-PIM:

Prerequisites

Before configuring IPv6 BIDIR-PIM, 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 address of a static RP and the IPv6 ACL that defines the range of IPv6 multicast groups to be served by the static RP
- Determine the C-RP priority and the IPv6 ACL that defines the range of IPv6 multicast groups to be served by each C-RP
- Determine the legal C-RP address range and the IPv6 ACL that defines the range of IPv6 multicast groups to be served
- 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

Because IPV6 BIDIR-PIM is implemented on the basis of IPv6 PIM-SM, you must enable IPv6 PIM-SM before enabling IPV6 BIDIR-PIM. To deploy an IPv6 BIDIR-PIM domain, enable IPv6 PIM-SM on all non-border interfaces of the domain.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enable IPv6 multicast routing.	**multicast ipv6 routing-enable**	Required. Disable by default.
3. Enter interface view.	**interface** *interface-type interface-number*	—
4. Enable IPv6 PIM-SM.	**pim ipv6 sm**	Required. Defaults to disabled.

All the interfaces of the same device must work in the same IPv6 PIM mode.

For more information about **multicast ipv6 routing-enable**, see *IP Multicast Command Reference*.

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.

CAUTION:

In an IPv6 PIM network, if both IPv6 PIM-SM and IPv6 BIDIR-PIM are enabled, do not configure the same RP to serve IPv6 PIM-SM and IPv6 BIDIR-PIM simultaneously to avoide IPv6 PIM routing table errors.

Configuring a static RP

If only one dynamic RP exists in a network, configuring a static RP can avoid communication interruption due to single-point failures and avoid frequent message exchange between C-RPs and the BSR. You must perform static RP configuration on all routers in the IPv6 PIM-SM domain and specify the same RP address. 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, specify a virtual IPv6 address, like 1001::100/64, for the static RP. As a result, the link becomes an RPL.

Perform this configuration on all routers in the IPv6 BIDIR-PIM domain.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure a static RP for IPv6 BIDIR-PIM.	**static-rp** *ipv6-rp-address* [*acl6-number*] [**preferred**] **bidir**	Required. 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 be served 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.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure an interface to be a C-RP for IPv6 BIDIR-PIM.	**c-rp** *ipv6-address* [{ **group-policy** *acl6-number* | **scope** *scope-id* } | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] * **bidir**	Required. No C-RP is configured by default.

When configuring a C-RP, ensure a relatively large bandwidth between this C-RP and the other devices in the IPv6 BIDIR-PIM domain.

An RP can serve multiple IPv6 multicast groups or all IPv6 multicast groups. Only one RP can forward multicast traffic for an IPv6 multicast group at a moment.

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.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Enable embedded RP.	**embedded-rp** [*acl6-number*]	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 the chapter "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. Upon 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure the C-RP-Adv interval.	**c-rp advertisement-interval** *interval*	Optional. Defaults to 60 seconds.
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 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 configuring 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 IP 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 in the priority exists, 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, but 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:

1. 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, a BSR can be protected against attacks from external hosts after you enable the border routers to perform neighbor checks and RPF checks on bootstrap messages and discard unwanted messages.
2. 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. However, if a legal BSR is controlled by an attacker, the mentioned problem will still occur.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter Ipv6 PIM view.	**pim ipv6**	—
3. Configure an interface as a C-BSR.	**c-bsr** *ipv6-address* [*hash-length* [*priority*]]	Required. No C-BSRs are configured by default.
4. Configure a legal BSR address range.	**bsr-policy** *acl6-number*	Optional. No restrictions on BSR address range by default.

Because a large amount of information needs to 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.

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 are intended to form the IPv6 BIDIR-PIM domain border.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure an IPv6 BIDIR-PIM domain border.	**pim ipv6 bsr-boundary**	Required. 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure the hash mask length.	**c-bsr hash-length** *hash-length*	Optional. 126 by default.
4. Configure the C-BSR priority.	**c-bsr priority** *priority*	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 it serves. 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 the BSR state times out and no bootstrap message is received from the BSR, a new BSR election process is triggered among the C-BSRs.

Perform the following configuration on C-BSR routers. Be sure to configure the BS period value smaller than the BS timeout value.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure the BS period.	**c-bsr interval** *interval*	Optional. For the default value, see the note under this table.
4. Configure the BS timeout.	**c-bsr holdtime** *interval*	Optional. For the default value, see the note under this table.

BS period and timeout settings

Make sure that the BS period value is smaller than the BS timeout value.

The BS period defaults to the value 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 timeout setting defaults to the value determined by the formula:

"BS timeout = BS period × 2 + 10". The default BS period is 60 seconds, so the default BS timeout = 60 × 2 + 10 = 130 (seconds)

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).

- Upon 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 upon 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.

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 do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Disable the BSM semantic fragmentation function.	**undo bsm-fragment enable**	Required. By default, the BSM semantic fragmentation function is enabled.

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.

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, partition the IPv6 BIDIR-PIM domain into multiple admin-scope zones. Each admin-scope zone maintains a BSR, which serves a specific multicast group range, and the global scope zone also maintains a BSR, which serves all the rest multicast groups.

Enabling IPv6 administrative scoping

Before configuring an IPv6 admin-scope zone, you must enable IPv6 administrative scoping first.

Perform the following configuration on routers that can become a C-BSR and ZBR.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Enable IPv6 administrative scoping.	**c-bsr admin-scope**	Required. Defaults to disabled.

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 serves 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 can become a ZBR.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure an IPv6 multicast forwarding boundary.	**multicast ipv6 boundary** { *ipv6-group-address prefix-length* | **scope** { *scope-id* | **admin-local** | **global** | **organization-local** | **site-local** } }	Required. By default, no IPv6 multicast forwarding boundary is configured.

For more information about **multicast ipv6 boundary** 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.

Perform the following configuration on the routers that will work as C-BSRs in admin-scope zones.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure a C-BSR for an admin-scope zone.	**c-bsr scope** { *scope-id* | **admin-local** | **global** | **organization-local** | **site-local** } [**hash-length** *hash-length* | **priority** *priority*] *	Required. No C-BSRs are configured for an admin-scope zone by default.

Hash mask length and C-BSR priority

You can configure these parameters at three levels:

- Global configuration level
- Global scope zone level
- Admin-scope zone level

Parameter values configured at the admin-scope zone level has preference over the global configuration level values, and default to the global value level.

For configuration of global C-BSR parameters, see "Configuring global C-BSR parameters."

Configuring IPv6 PIM-SSM

The IPv6 PIM-SSM model needs the support of MLDv2. Therefore, be sure to enable MLDv2 on IPv6 PIM routers with receivers attached to them.

Prerequisites

Before configuring IPv6 PIM-SSM, complete the following tasks:

- Enable IPv6 forwarding and configure any 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

The SSM model is implemented based on some subsets of IPv6 PIM-SM. Therefore, a router is IPv6 PIM-SSM capable after you enable IPv6 PIM-SM on it.

When you deploy an IPv6 PIM-SM domain, enable IPv6 PIM-SM on all non-border interfaces of routers.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enable IPv6 multicast routing.	**multicast ipv6 routing-enable**	Required. Disable by default.
3. Enter interface view.	**interface** *interface-type interface-number*	—
4. Enable IPv6 PIM-SM.	**pim ipv6 sm**	Required. Defaults to disabled.

ll interfaces of the same device must work in the same IPv6 PIM mode. For more information about **multicast ipv6 routing-enable**, see *IP Multicast Command Reference*.

Configuring the IPv6 SSM group range

As for 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, this depends on whether the group address in the (S, G) channel subscribed by the receivers falls in 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.

Perform the following configuration on all routers in the IPv6 PIM-SM domain.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure the IPv6 SSM group range.	**ssm-policy** *acl6-number*	Optional. FF3x::/32 by default, here "x" refers to any legal group scope.

Make sure that 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.

Configuring IPv6 PIM common features

Prerequisites

Before configuring IPv6 PIM common features, complete the following tasks:

- Enable IPv6 forwarding and configure any IPv6 unicast routing protocol so that all devices in the domain are interoperable at the network layer
- Configure IPv6 PIM-DM, IPv6 PIM-SM or IPv6 PIM-SSM
- Determine the IPv6 ACL for filtering IPv6 multicast data
- Determine the IPv6 ACL that defins 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

Configuring an IPv6 multicast data filter

No matter in 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.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure an IPv6 multicast group filter.	**source-policy** *acl6-number*	Required. No IPv6 multicast data filter by default.

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.

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 guard 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 do...	Use the command...	Remarks
1. Enter system view	**system-view**	—
2. Enter interface view	**interface** *interface-type interface-number*	—
3. Configure a hello message filter	**pim ipv6 neighbor-policy** *acl6-number*	Required. No hello message filter by default.

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 both an IPv6 PIM-DM domain and an IPv6 PIM-SM domain, the hello messages sent among routers contain many configurable options, including:

- DR_Priority—Priority for DR election for IPv6 PIM-SM only. 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—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—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 will take effect. If you want to enable neighbor tracking on a router, be sure to enable the neighbor tracking feature on all IPv6 PIM routers on a multi-access subnet.

The LAN-delay setting causes the upstream routers to delay processing received prune messages. The override-interval sets the length of time that a downstream router will 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 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-enabled routers on the same multi-access subnet. Otherwise, the upstream router will fail to explicitly track which downstream routers have joined to it.

Configuring hello options globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure the priority for DR election.	**hello-option dr-priority** *priority*	Optional. 1 by default.
4. Configure IPv6 PIM neighbor timeout time.	**hello-option holdtime** *interval*	Optional. Defaults to 105 seconds.

To do...	Use the command...	Remarks
5. Configure the prune message delay time (LAN-delay).	**hello-option lan-delay** *interval*	Optional. 500 milliseconds by default.
6. Configure the prune override interval.	**hello-option override-interval** *interval*	Optional. 2,500 milliseconds by default.
7. Disable join suppression.	**hello-option neighbor-tracking**	Required. Enabled by default.

Configuring hello options on an interface

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure the priority for DR election.	**pim ipv6 hello-option dr-priority** *priority*	Optional. 1 by default.
4. Configure IPv6 PIM neighbor timeout time.	**pim ipv6 hello-option holdtime** *interval*	Optional. Defaults to 105 seconds.
5. Configure the prune message delay time (LAN-delay).	**pim ipv6 hello-option lan-delay** *interval*	Optional. 500 milliseconds by default.
6. Configure the prune override interval.	**pim ipv6 hello-option override-interval** *interval*	Optional. 2,500 milliseconds by default.
7. Disable join suppression.	**pim ipv6 hello-option neighbor-tracking**	Required. Enabled by default.
8. Configure the interface to reject hello messages without a generation ID.	**pim ipv6 require-genid**	Required. By default, hello messages without Generation_ID are accepted.

Configuring the prune delay

If a downstream router on a multi-access LAN does not support the prune override interval option, configure the **prune delay** time on the upstream router so that it will not perform the prune action immediately after receiving the prune message. Instead, it maintains the current forwarding state for a period of prune delay time. In this period, if the upstream router receives a join message from the downstream router, it cancels the prune action.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure the prune delay interval.	**prune delay** *interval*	Optional. 3 seconds by default.

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.

Upon 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.

Configuring IPv6 PIM common timers globally

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure the hello interval.	**timer hello** *interval*	Optional. Defaults to 30 seconds.
4. Configure the join/prune interval.	**timer join-prune** *interval*	Optional. Defaults to 60 seconds.
5. Configure the join/prune timeout time.	**holdtime join-prune** *interval*	Optional. Defaults to 210 seconds.
6. Configure assert timeout time.	**holdtime assert** *interval*	Optional. Defaults to 180 seconds.
7. Configure the IPv6 multicast source lifetime.	**source-lifetime** *interval*	Optional. Defaults to 210 seconds.

Configuring IPv6 PIM common timers on an interface

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Configure the hello interval.	**pim ipv6 timer hello** *interval*	Optional. Defaults to 30 seconds.
4. Configure the maximum delay between hello messages.	**pim ipv6 triggered-hello-delay** *interval*	Optional. Defaults to 5 seconds.

To do...	Use the command...	Remarks
5. Configure the join/prune interval.	**pim ipv6 timer join-prune** *interval*	Optional. Defaults to 60 seconds.
6. Configure the join/prune timeout time.	**pim ipv6 holdtime join-prune** *interval*	Optional. Defaults to 210 seconds.
7. Configure assert timeout time.	**pim ipv6 holdtime assert** *interval*	Optional. Defaults to 180 seconds.

If there are no special networking requirements, we recommend that you use the default settings.

Configuring join/prune message sizes

A larger join/prune message size will result in loss of a larger amount of information when a message is lost. With a reduced join/message size, the loss of a single message will bring a relatively minor impact.

The maximum number of (S, G) entries in a join/prune message can reduce the number of (S, G) entries sent per unit of time.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter IPv6 PIM view.	**pim ipv6**	—
3. Configure the maximum size of a join/prune message.	**jp-pkt-size** *packet-size*	Optional. 8,100 bytes by default.
4. Configure the maximum number of (S, G) entries in a join/prune message.	**jp-queue-size** *queue-size*	Optional. 1,020 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 origianl 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 configuring this feature on an interface, be sure to enable IPv6 PIM-DM or IPv6 PIM-SM on the interface. For more information about BFD, see *High Availability Configuration Guide*.

To do...	Use the commad...	Remarks
1. Enter system view.	**system-view**	—
2. Enter interface view.	**interface** *interface-type interface-number*	—
3. Enable IPv6 PIM to work with BFD.	**pim ipv6 bfd enable**	Required. Defaults to disabled.

Displaying and maintaining IPv6 PIM

To do...	Use the command...	Remarks
View 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** } *regular-expression*]	Available in any view.
View the information of IPv6 unicast routes used by IPv6 PIM.	**display pim ipv6 claimed-route** [*ipv6-source-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
View the number of IPv6 PIM control messages.	**display pim ipv6 control-message counters** [**message-type** { **probe** | **register** | **register-stop** } | [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **crp** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** }] *] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the DF information of IPv6 BIDIR-PIM.	**display pim ipv6 df-info** [*rp-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
View the information about unacknowledged graft messages.	**display pim ipv6 grafts** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
View the IPv6 PIM information on an interface or all interfaces.	**display pim ipv6 interface** [*interface-type interface-number*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
View the information of join/prune messages to send.	**display pim ipv6 join-prune mode** { **sm** [**flags** *flag-value*] | **ssm** } [**interface** *interface-type interface-number* | **neighbor** *ipv6-neighbor-address*] * [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
View IPv6 PIM neighboring information.	**display pim ipv6 neighbor** [**interface** *interface-type interface-number* | *ipv6-neighbor-address* | **verbose**] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
View the content of the IPv6 PIM routing table.	**display pim ipv6 routing-table** [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **incoming-interface** [*interface-type interface-number* | **register**] | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** } | **mode** *mode-type* | **flags** *flag-value* | **fsm**] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
View the RP information.	**display pim ipv6 rp-info** [*ipv6-group-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Reset IPv6 PIM control message counters.	**reset pim ipv6 control-message counters** [**interface** *interface-type interface-number*]	Available in user view.

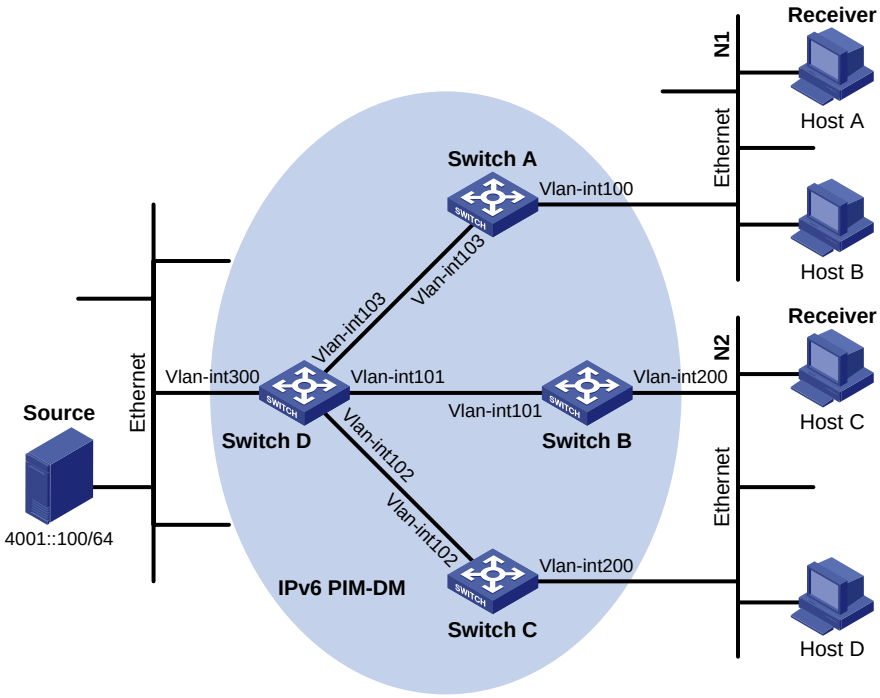
IPv6 PIM configuration examples

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 operates in the dense mode.
- Host A and Host Care multicast receivers in the stub networks N1 and N2.
- Switch D connects to the network that comprises the multicast source (Source) through VLAN-interface 300.
- Switch A connects to N1 through VLAN-interface 100, and to Switch D through VLAN-interface 103.
- Switch B and Switch C connect to N2 through their respective VLAN-interface 200, and to Switch D through VLAN-interface 101 and VLAN-interface 102 respectively.
- MLDv1 will run between Switch A and N1, and between Switch B/Switch C and N2.

Figure 112 Network diagram for IPv6 PIM-DM configuration



Device	Interface	IP address	Device	Interface	IP 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			

Procedure

1. Enable IPv6 forwarding and configure IPv6 addresses and IPv6 unicast routing

Enable IPv6 forwarding on each switch and configure the IPv6 address and prefix length for each interface as shown in Figure 112. Detailed configuration steps are omitted here.

Configure OSPFv3 on the switches in the IPv6 PIM-DM domain to ensure network-layer reachability among them. Detailed configuration steps are omitted here.

2. Enable IPv6 multicast routing, and enable IPv6 PIM-DM and MLD

Enable IPv6 multicast routing on Switch A, enable IPv6 PIM-DM on each interface, and enable MLD on VLAN-interface 100, which connects Switch A to N1.

```
<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
```

The configuration on Switch B and Switch C is similar to that on Switch A.

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
```

3. Verify the configuration

Use **display pim ipv6 interface** to view the IPv6 PIM configuration and running status on each interface. For example:

View the IPv6 PIM configuration information on Switch D.

```
[SwitchD] display pim ipv6 interface
 Interface          NbrCnt HelloInt   DR-Pri     DR-Address
 Vlan300            0      30         1          4001::1
                                                 (local)
 Vlan103            0      30         1          1002::2
                                                 (local)
 Vlan101            1      30         1          2002::2
```

```
                                                  (local)
 Vlan102            1      30         1           3001::2
                                                  (local)
```

Use **display pim ipv6 neighbor** to view the IPv6 PIM neighboring relationships among the switches. For example:

View the IPv6 PIM neighboring relationships on Switch D.

```
[SwitchD] display pim ipv6 neighbor
 Total Number of Neighbors = 3

 Neighbor           Interface           Uptime   Expires  Dr-Priority
 1002::1            Vlan103             00:04:00 00:01:29 1
 2002::1            Vlan101             00:04:16 00:01:29 3
 3001::1            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. Use the **display pim IPv6 routing-table** command to view the IPv6 PIM routing table information on each switch. For example:

View the 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
```

The output on Switch B and Switch C is similar to that on Switch A.

View the IPv6 PIM multicast routing table information on Switch D.

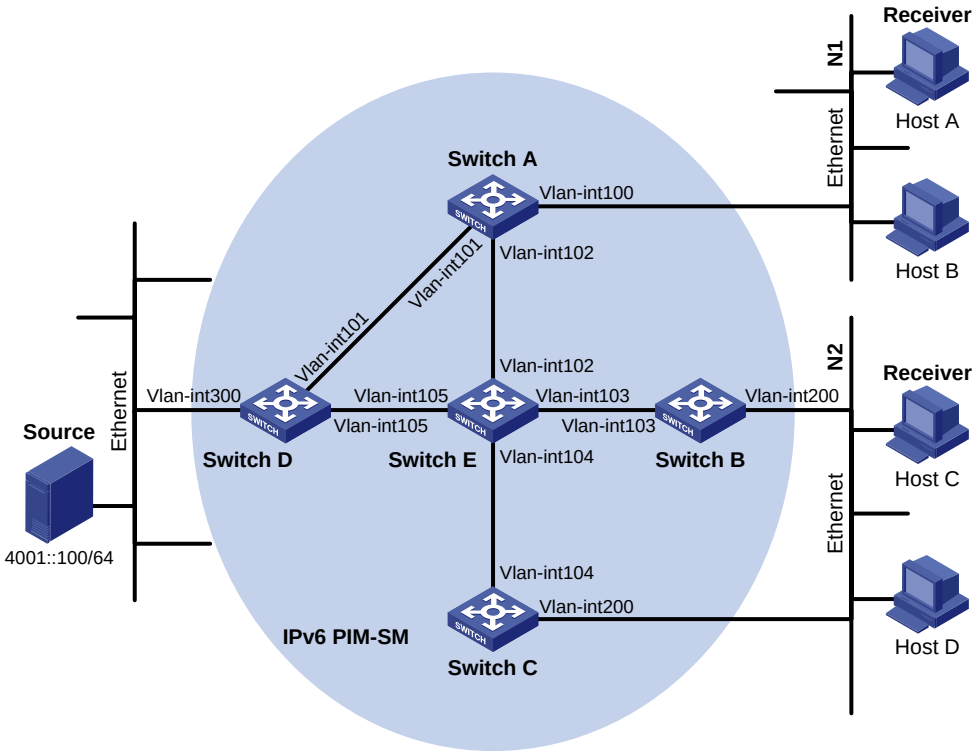
```
[SwitchD] display pim ipv6 routing-table
 Total 0 (*, G) entry; 1 (S, G) entry

 (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: 3
         1: Vlan-interface103
             Protocol: pim-dm, UpTime: 00:02:19, Expires: never
         2: Vlan-interface101
             Protocol: pim-dm, UpTime: 00:02:19, Expires: never
         3: 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 operates in the sparse mode.
- Host A and Host C are IPv6 multicast receivers in two stub networks N1 and N2.
- Switch D connects to the network that comprises the IPv6 multicast source through VLAN-interface 300.
- Switch A connects to N1 through VLAN-interface 100, and to Switch D and Switch E through VLAN-interface 101 and VLAN-interface 102 respectively.
- Switch B and Switch C connect to N2 through their respective VLAN-interface 200, and to Switch E through VLAN-interface 103 and VLAN-interface 104 respectively.
- 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 served by the C-RP is FF0E::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 113 Network diagram for IPv6 PIM-SM non-scoped zone configuration



Device	Interface	IP address	Device	Interface	IP 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

Procedure

1. Enable IPv6 forwarding and configure IPv6 addresses and IPv6 unicast routing

Enable IPv6 forwarding on each switch and configure the IPv6 address and prefix length for each interface as shown in Figure 113. Detailed configuration steps are omitted here.

Configure OSPFv3 on the switches in the IPv6 PIM-DM domain to ensure network-layer reachability among them. Detailed configuration steps are omitted here.

2. Enable IPv6 multicast routing, and enable IPv6 PIM-SM and MLD

Enable IPv6 multicast routing on Switch A, enable IPv6 PIM-SM on each interface, and enable MLD on VLAN-interface 300, which connects Switch A to N1.

```
<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
```

The configuration on Switch B and Switch C is similar to that on Switch A. The configuration on Switch D and Switch E is also similar to that on Switch A except that it is not necessary to enable MLD on the corresponding interfaces on these two switches.

3. 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
```

4. Verify the configuration

Use **display pim ipv6 interface** to view the IPv6 PIM configuration and running status on each interface. For example:

View the 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         1001::1
                                                   (local)
 Vlan101              1      30         1         1002::2
 Vlan102              1      30         1         1003::2
```

To view the BSR election information and the locally configured C-RP information in effect on a switch, use **display pim ipv6 bsr-info**. For example:

View the BSR information and the locally configured C-RP information 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
```

View the BSR information and the locally configured C-RP information 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
```

View the BSR information and the locally configured C-RP information 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
```

To view the RP information discovered on a switch, use **display pim ipv6 rp-info**. For example:

View the 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. Upon 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. Use **display pim ipv6 routing-table** to view the PIM routing table information on the switches. For example:

View the 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
```

The output on Switch B and Switch C is similar to that on Switch A.

View the 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
```

View the 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

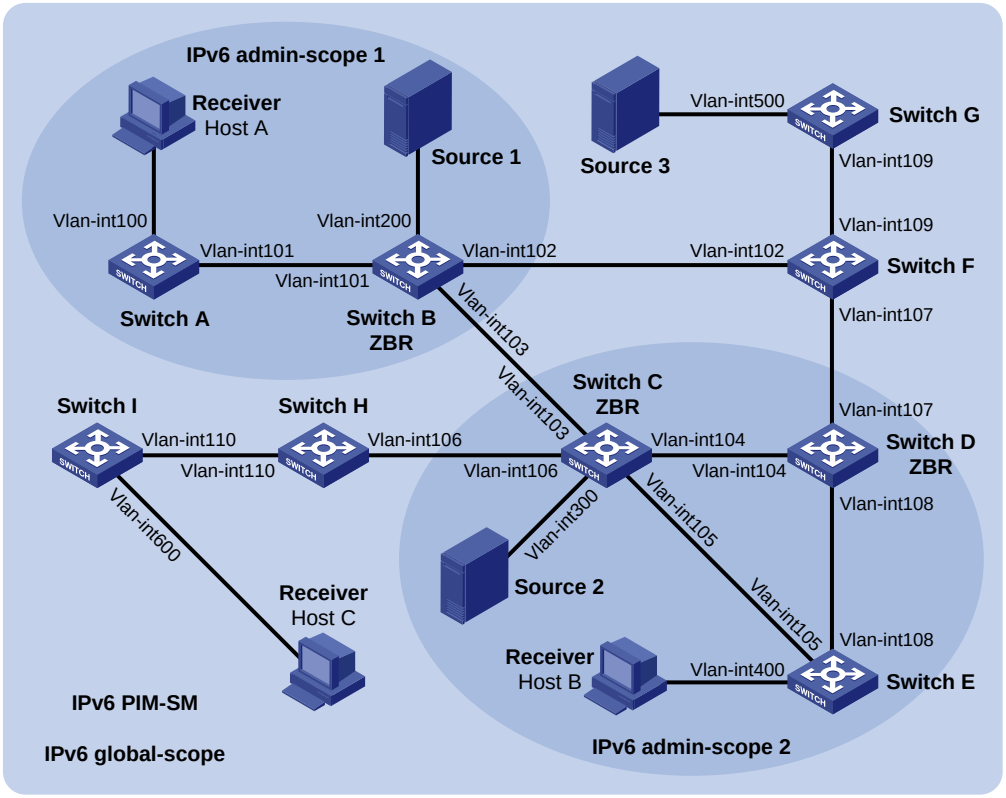
Network requirements

- 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 from only Source 1, and Host B receives the multicast information from only 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 serve 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 serve 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 serve IPv6 multicast groups with the Scope field value in their group addresses being 14.

- MLDv1 is required between Switch A, Switch E, Switch I and their respective receivers.

Network diagram

Figure 114 Network diagram for IPv6 PIM-SM admin-scope zone configuration



Device	Interface	IP address	Device	Interface	IP 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		Vlan-int107	6002::1/64
	Vlan-int101	1002::2/64	Switch E	Vlan-int400	7001::1/64
	Vlan-int103	2002::1/64		Vlan-int105	3003::2/64
	Vlan-int102	2003::1/64		Vlan-int108	6001::2/64
Switch C	Vlan-int300	3001::1/64	Switch F	Vlan-int109	8001::1/64
	Vlan-int104	3002::1/64		Vlan-int107	6002::2/64
	Vlan-int105	3003::1/64		Vlan-int102	2003::2/64
	Vlan-int103	2002::2/64	Switch G	Vlan-int500	9001::1/64
	Vlan-int106	3004::1/64		Vlan-int109	8001::2/64
Switch H	Vlan-int110	4001::1/64	Source 1	—	2001::100/64
	Vlan-int106	3004::2/64	Source 2	—	3001::100/64
Switch I	Vlan-int600	5001::1/64	Source 3	—	9001::100/64
	Vlan-int110	4001::2/64			

Procedure

1. Configure IPv6 addresses and unicast routing

Configure the IPv6 address and prefix length for each interface as shown in Figure 114. The detailed configuration steps are omitted here.

Configure OSPFv3 on the switches in the IPv6 PIM-SM domain to ensure network-layer reachability among them. Detailed configuration steps are omitted here.

2. 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 IPv6 PIM-SM on each interface, and enable MLD on the host-side interface VLAN-interface 100.

```
<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
```

The configuration on Switch E and Switch I is similar to the configuration on Switch A.

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
```

The configuration on Switch C, Switch D, Switch F, Switch G, and Switch H is similar to the configuration on Switch B. The specific configuration steps are omitted here.

3. 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
```

4. 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
```

5. Verify the configuration

To view the BSR election information and the C-RP information on a switch, use **display pim ipv6 bsr-info**. For example:

View the BSR information and the locally configured C-RP information 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
```

View the BSR information and the locally configured C-RP information 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
```

View the BSR information and the locally configured C-RP information 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 **display pim ipv6 rp-info**. For example:

View the 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
```

View the 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
```

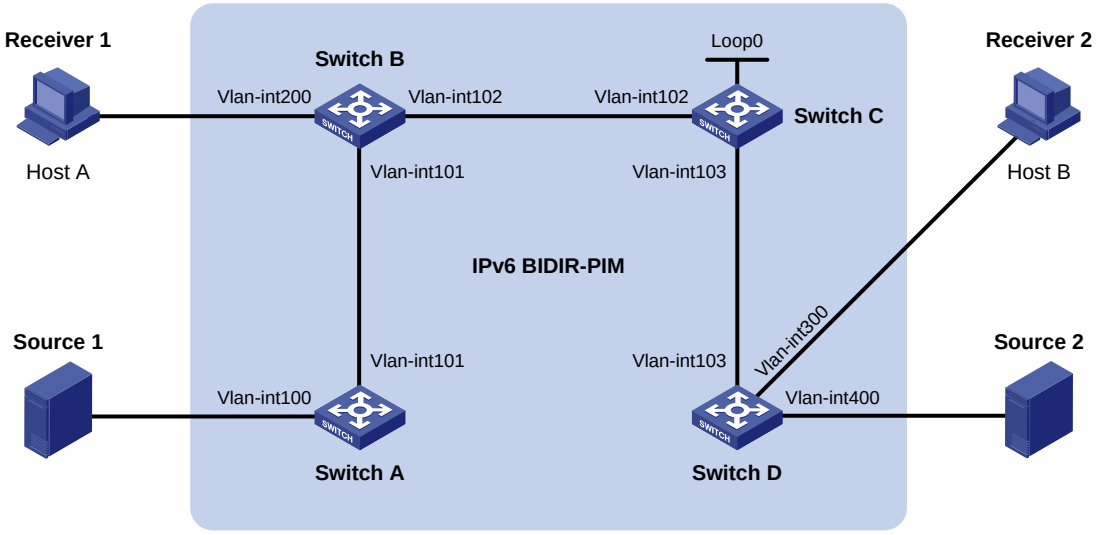
```
prefix/prefix length: FFBE::/16
    RP: 8001::1
    Priority: 192
    HoldTime: 130
    Uptime: 00:03:39
    Expires: 00:01:51

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 in Figure 115. Source 1 and Source 2 send different multicast information to IPv6 multicast group FF14::101. 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 acts as a C-RP of the IPv6 BIDIR-PIM domain.
- IGMPv2 will run between Switch B and Host A, and between Switch D and Host B.

Figure 115 Network diagram for IPv6 BIDIR-PIM configuration



Device	Interface	IP address	Device	Interface	IP 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			

Procedure

1. Configure IPv6 forwarding, IPv6 addresses and IPv6 unicast routing protocol

Enable IPv6 forwarding on each switch, and and configure IPv6 address and prefix length for each interface as shown in Figure 115. The configuration steps are omitted here.

Configure OSPF on the switches in the IPv6 BIDIR-PIM domain to ensure network-layer reachability among them. The configuration steps are omitted here.

2. 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 on 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 on 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
```

3. Configure C-BSR and C-RP

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
```

4. Verify the configuration

To view the DF information of IPv6 BIDIR-PIM on a switch, use **display pim ipv6 df-info**:

View 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
```

View 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
```

View 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)
```

View 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
```

To view the DF information of the IPv6 multicast forwarding table on a switch, use **display multicast ipv6 forwarding-table df-info**. For more information about this command, see the *IP Multicast Command Reference*.

View 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
```

View 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
```

View 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
```

View the DF information of the IPv6 multicast forwarding table on Switch D.

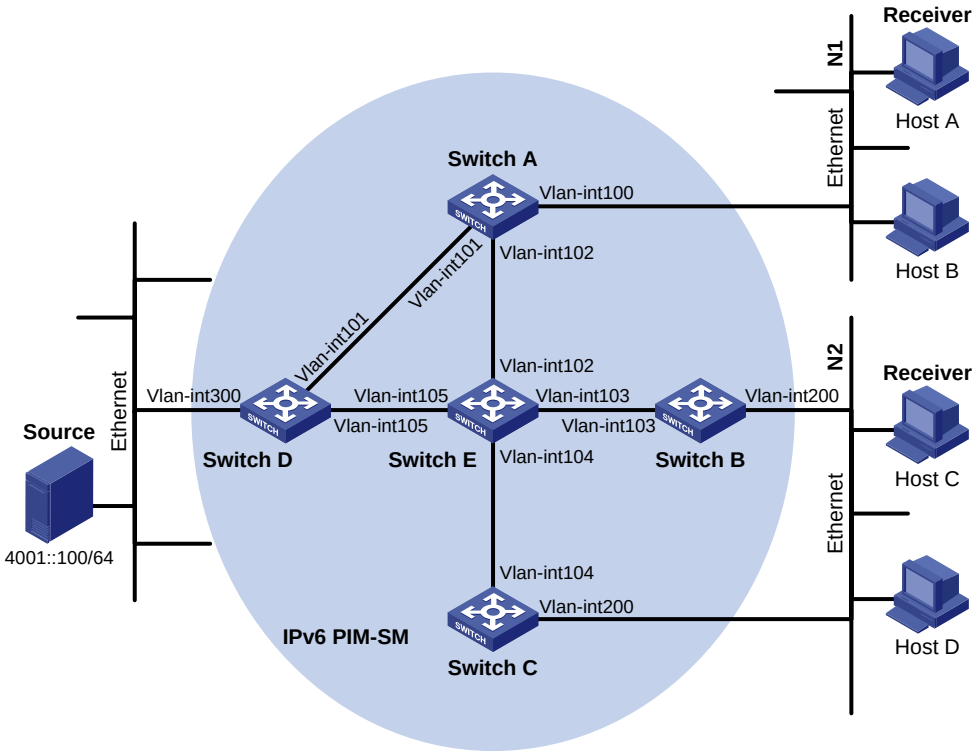
```
[SwitchD] display multicast ipv6 forwarding-table df-info
Multicast DF information
Total 1 RP

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 operates in the SSM mode.
- Host A and Host C are IPv6 multicast receivers in two stub networks N1 and N2.
- Switch D connects to the network that comprises the IPv6 multicast source through VLAN-interface 300.
- Switch A connects to N1 through VLAN-interface 100, and to Switch D and Switch E through VLAN-interface 101 and VLAN-interface 102 respectively.
- Switch B and Switch C connect to N2 through their respective VLAN-interface 200, and to Switch E through VLAN-interface 103 and VLAN-interface 104 respectively.
- Switch E connects to Switch A, Switch B, Switch C and Switch D.
- The SSM group range is FF3E::/64.
- MLDv2 runs between Switch A and N1, and between Switch B/Switch C and N2.

Figure 116 Network diagram for IPv6 PIM-SSM configuration



Device	Interface	IP address	Device	Interface	IP 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

Procedure

1. Enable IPv6 forwarding and configure IPv6 addresses and IPv6 unicast routing

Enable IPv6 forwarding on each switch and configure the IPv6 address and prefix length for each interface as shown in Figure 116. Detailed configuration steps are omitted here.

Configure OSPFv3 on the switches in the IPv6 PIM-DM domain to ensure network-layer reachability among them. Detailed configuration steps are omitted here.

2. Enable IPv6 multicast routing, and enable IPv6 PIM-SM and MLD

Enable IPv6 multicast routing on Switch A, enable IPv6 PIM-SM on each interface, and run MLDv2 on VLAN-interface 100, which connects Switch A to N1.

```
<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
```

The configuration on Switch B and Switch C is similar to that on Switch A. The configuration on Switch D and Switch E is also similar to that on Switch A except that it is not necessary to enable MLD on the corresponding interfaces on these two switches.

3. 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
```

The configuration on Switch B, Switch C, Switch D, and Switch E is similar to that on Switch A.

4. Verify the configuration

Use **display pim ipv6 interface** to view the IPv6 PIM configuration and running status on each interface. For example:

View the IPv6 PIM configuration information on Switch A.

```
[SwitchA] display pim ipv6 interface
 Interface             NbrCnt HelloInt   DR-Pri   DR-Address
 Vlan100               0      30         1        1001::1
                                                  (local)
 Vlan101               1      30         1        1002::2
 Vlan102               1      30         1        1003::2
```

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. The switches on the SPT path (Switch A and Switch D) have generated an (S, G) entry, and Switch E, which is not on the SPT path, does not have IPv6 multicast routing entries. Use **display pim ipv6 routing-table** to view the IPv6 PIM routing table information on each switch. For example:

View the 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
```

The output on Switch B and Switch C is similar to that on Switch A.

View the 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 of building a multicast distribution tree correctly

Symptom

None of the routers in the network (including routers directly connected with IPv6 multicast sources and receivers) has 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 surely 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 surely fail, resulting in abnormal multicast forwarding.

Solution

1. Evaluate IPv6 unicast routes. Use **display ipv6 routing-table** to determine whether a unicast route exists to the IPv6 multicast source or the RP.
2. Verify that the RPF interface is IPv6 PIM enabled. Use **display pim ipv6 interface** to view the IPv6 PIM information on each interface. If IPv6 PIM is not enabled on the interface, use **pim ipv6 dm** or **pim ipv6 sm** to enable IPv6 PIM.

3. Verify that the RPF neighbor is an IPv6 PIM neighbor. Use **display pim ipv6 neighbor** to view the PIM neighbor information.
4. Verify that IPv6 PIM and MLD are enabled on the interfaces that directly connect to the IPv6 multicast source and to the receiver.
5. Verify that the same IPv6 PIM mode is enabled on related interfaces. Use **display pim ipv6 interface verbose** to determine whether the same PIM mode is enabled on the RPF interface and the corresponding interface of the RPF neighbor router.
6. Verify that the same IPv6 PIM mode is enabled on all the routers in the entire network. Use **display current-configuration** to view the IPv6 PIM mode information on each interface. 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 **multicast ipv6 boundary**, any IPv6 multicast packet will be kept from crossing the boundary, and therefore no routing entry can be created in the IPv6 PIM routing table.
- In addition, **source-policy** filters received IPv6 multicast packets. If the IPv6 multicast data fails to pass the ACL rule defined in this command, IPv6 PIM cannot create the route entry, either.

Solution

1. Verify the IPv6 multicast forwarding boundary configuration. Use **display current-configuration** to view the IPv6 multicast forwarding boundary settings. Use **multicast ipv6 boundary** to change the IPv6 multicast forwarding boundary settings.
2. Verify the IPv6 multicast filter configuration. Use **display current-configuration** to view the IPv6 multicast filter configuration. Change the IPv6 ACL rule defined in **source-policy** so that the source/group address of the IPv6 multicast data can pass ACL filtering.

RPs unable to 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 serves 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 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. Verify that a route is available to the RP. Use **display ipv6 routing-table** to determine whether a route is available on each router to the RP.
2. Evaluate the dynamic RP information. Use **display pim ipv6 rp-info** to determine whether the RP information is consistent on all routers. In the case of inconsistent RP information, configure consistent RP address on all the routers.
3. Evaluate the static RP configuration. Use **display pim ipv6 rp-info** to determine whether 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 register 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 will be unable to receive the advertisements from the C-RP, and therefore 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. Verify that the routes to C-RPs, the RP and the BSR are available. Use **display ipv6 routing-table** to determine whether the routes to the RP and the BSR are available on each router, and whether a route is available between the RP and the BSR. Be 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. Evaluate the RP and BSR information. IPv6 PIM-SM needs the support of the RP and BSR. Use **display pim ipv6 bsr-info** to determine whether the BSR information is available on each router, and then use **display pim ipv6 rp-info** to determine whether the RP information is correct.
3. View the IPv6 PIM neighboring relationships. Use **display pim ipv6 neighbor** to determine whether the normal neighboring relationships have been established among the routers.

Configuring IPv6 MBGP configuration

BGP-4 can carry routing information for IPv4 only. IETF defined MBGP extensions to carry routing information for multiple network layer protocols.

On an IPv6 network, the IPv6 multicast topology must be different from the IPv6 unicast topology. To meet the requirement, the MBGP extensions enable IPv6 BGP to carry the IPv6 unicast NLRI and IPv6 multicast NLRI separately, and the multicast NLRI performs RPF exclusively. In this way, route selection for a destination through the IPv6 unicast routing table and through the IPv6 multicast routing table will have different results, ensuring the normal unicast and multicast operation across ASs.

MBGP is defined in RFC 2858 (Multiprotocol Extensions for BGP-4).

MBGP for IPv6 multicast is called "IPv6 MBGP.

This document covers configuration tasks related to multi-protocol BGP for IPv6 multicast only. For BGP related information, see *BGP* in the *Layer 3 – IP Routing Configuration Guide*.

For information about RPF, see *IP Multicast Configuration Guide*.

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

This chapter describes only configuration for IPv6 MBGP. For IPv6 BGP related information, see *Layer 3 – IP Routing Configuration Guide*.

Configuring IPv6 MBGP basic functions

Prerequisites

IPv6 MBGP is an application of multi-protocol BGP. Therefore, before configuring IPv6 MBGP, configure IPv6 MBGP, complete the following tasks:

- Enable IPv6.
- Configure network layer addresses for interfaces.
- Complete BGP basic configuration.

Configuring an IPv6 MBGP peer

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enable BGP and enter BGP view.	**bgp** *as-number*	Required. Not enabled by default.
3. Enter IPv6 address family view.	**ipv6-family**	—
4. Specify a IPv6 BGP peer and its AS number.	**peer** *ipv6-address* **as-number** *as-number*	Required. Not configured by default.
5. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—

To do...	Use the command...	Remarks
6. Enable the IPv6 MBGP peer.	**peer** *ipv6-address* **enable**	Required. Not enabled by default.

Configuring a preferred value for routes from a peer/peer group

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
4. Specify a preferred value for routes received from the IPv6 MBGP peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **preferred-value** *value*	Optional. The preferred value defaults to 0.

If you reference a routing policy and use **peer** { *ipv6-group-name* | *ipv6-address* } **preferred-value** *value* to set a preferred value for routes from a peer or peer group, the routing policy sets the specific preferred value for matching routes. Routes that do not match the routing policy use the value set with the **peer** command.

If the preferred value in the routing policy is zero, the matching routes also use the value set with **peer** { *ipv6-group-name* | *ipv6-address* } **preferred-value** *value*. For information on using a routing policy to set a preferred value, see *Layer 3 – IP Routing Command Reference*.

Controlling route distribution and reception

Prerequisites

Before configuring IPV6 MBGP, complete the following tasks:

- Enable IPv6.
- Configure the IPv6 MBGP basic functions

Injecting a local IPv6 MBGP route

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
4. Inject a network to the IPv6 MBGP routing table.	**network** *ipv6-address prefix-length* [**route-policy** *route-policy-name* | **short-cut**]	Required. Not injected by default.

Configuring IPv6 MBGP route redistribution

To do…	Use the command…	Description
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP multicast address family view.	**ipv6-family multicast**	—
4. Enable default route redistribution into the IPv6 MBGP routing table.	**default-route imported**	Optional. By default, default route redistribution is not allowed.
5. Enable route redistribution from another routing protocol.	**import-route** *protocol* [*process-id* [**med** *med-value* | **route-policy** *route-policy-name*] *]	Required. Not enabled by default.

If the **default-route imported** command is not configured, using the **import-route** command cannot redistribute any IGP default route.

Configuring IPv6 MBGP route summarization

To reduce the routing table size on medium and large BGP networks, configure route summarization on IPv6 MBGP routers. BGP supports only manual summarization of IPv6 multicast routes.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
4. Configure manual route summarization.	**aggregate** *ipv6-address prefix-length* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*]*	Required. Not configured by default.

Advertising a default route to a peer or peer group

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
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*]	Required. Not advertised by default.

With the **peer default-route-advertise** command executed, the router sends a default route with the next hop being itself to the specified IPv6 MBGP peer/peer group, regardless of whether the default route is available in the routing table.

Configuring outbound IPv6 MBGP route filtering

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
4. Configure the filtering of outgoing routes.	**filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol process-id*]	Use any of the commands. No filtering is configured by default. Configure filter policies as needed. If you configure multiple filter policies, they will be applied in the following order: • filter-policy export • peer filter-policy export • peer as-path-acl export • peer ipv6-prefix export • peer route-policy export A filter policy can be applied only after the previous one is passed; routing information can be advertised only after passing all the filter policies configured.
5. Specify an IPv6 ACL to filter routes advertised to a peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **filter-policy** *acl6-number* **export**	
6. Specify an AS path ACL to filter IPv6 MBGP routing information advertised to a peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **as-path-acl** *as-path-acl-number* **export**	
7. Specify an IPv6 prefix list to filter routes advertised to a peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **ipv6-prefix** *ipv6-prefix-name* **export**	
8. Apply a routing policy to routes advertised to a peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **route-policy** *route-policy-name* **export**	

Members of an IPv6 MBGP peer group must have the same outbound route filtering policy as the peer group.

IPv6 BGP advertises redistributed routes passing the specified policy to the IPv6 MBGP peer.

Configuring inbound IPv6 MBGP route filtering

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
4. Configure inbound route filtering.	**filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**	Use any of the commands. By default, advertised routes are not filtered. Configure a filtering policy as
5. Apply a routing policy to routes from a peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **route-policy** *route-policy-name* **import**	

To do...	Use the command...	Remarks
6. Specify an IPv6 ACL to filter routes from a peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **filter-policy** *acl6-number* **import**	needed. 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 A filter policy can be applied only after the previous one is passed; routing information can be received only after passing all the filter policies configured.
7. Specify an AS path ACL to filter IPv6 BGP routing information from a peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **as-path-acl** *as-path-acl-number* **import**	
8. Specify an IPv6 prefix list to filter routes from a peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **ipv6-prefix** *ipv6-prefix-name* **import**	
9. Specify the upper limit of prefixes that can be imported from a peer/peer group	**peer** { *ipv6-group-name* | *ipv6-address* } **route-limit** *limit* [*percentage*]	Optional. The number is unlimited by default.

A peer has 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

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
4. Configure IPv6 MBGP route dampening parameters.	**dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*]*	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

Prerequisites

Before configuring IPv6 MBGP route attributes, complete the following tasks:

- Enable IPv6.
- Configure the IPv6 MBGP basic functions.

Configuring IPv6 MBGP route preferences

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
4. Configure preferences for external, internal, local IPv6 MBGP routes	**preference** { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }	Optional. The default preference values of external, internal and local routes are 255, 255, and 130, respectively.

Configuring the default local preference

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
4. Set the default local preference.	**default local-preference** *value*	Optional. By default, the default local preference is 100.

Configuring the MED attribute

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
4. Configure a default MED value.	**default med** *med-value*	Optional. By default, the default *med-value* is 0.
5. Enable the comparison of the MED for routes from different Ass.	**compare-different-as-med**	Optional. Not enabled by default

To do...	Use the command...	Remarks
6. Enable the comparison of the MED for routes from each AS.	**bestroute compare-med**	Optional. Defaults to disabled.
7. Enable the comparison of the MED for routes from confederation peers.	**bestroute med-confederation**	Optional Defaults to disabled.

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 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 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
4. Configure the router as the next hop of routes sent to the peer/peer group	**peer** { *ipv6-group-name* | *ipv6-address* } **next-hop-local**	Optional. By default, IPv6 MBGP specifies the local router as the next hop for routes sent to an eBGP peer/peer group, but not for routes sent to an iBGP peer/peer group.

Configuring the AS_PATH attribute

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
4. Allow the local AS number to appear in the AS-PATH of routes from a peer/peer group and specify the number of times that the local AS number can appear in the AS-PATH of routes from the peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **allow-as-loop** [*number*]	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.

To do…	Use the command…	Remarks
6. Configure updates to a peer/peer group to carry only the public AS number.	**peer** { *ipv6-group-name* | *ipv6-address* } **public-as-only**	Optional. By default, outbound IPv6 MBGP updates can carry private AS numbers.

Tuning and optimizing IPv6 MBGP networks

Prerequisites

Before tuning and optimizing an OSPF network, complete the following tasks:

- Enable IPv6.
- Configure the IPv6 MBGP basic functions.

Configuring IPv6 MBGP soft reset

After modifying a route selection policy, 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.

However, if a peer that does not support route refresh exists in the network, 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.

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 do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 address family view	**ipv6-family**	—
4. Enable IPv6 BGP route refresh for a peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **capability-advertise route-refresh**	Optional. Enabled by default.

Perform a manual soft-reset

If the peer does not support route refresh, 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 do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 address family view.	**ipv6-family**	—
4. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
5. Keep all routes from a peer/peer group regardless of whether they pass the inbound filtering policy.	**peer** { *ipv6-group-name* | *ipv6-address* } **keep-all-routes**	Required. Not kept by default.
6. Soft-reset IPv6 MBGP connections manually.	**refresh bgp ipv6 multicast** { **all** | *ipv6-address* | **group** *ipv6-group-name* | **external** | **internal** } { **export** | **import** }	Optional.

Enabling the IPv6 MBGP ORF capability

The BGP ORF feature allows 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 BGP 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 19.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	Required.
3. Enter IPv6 address family view.	**ipv6-family**	—
4. Enable BGP route refresh for a peer/peer group.	**peer** { *group-name* | *ipv6-address* } **capability-advertise route-refresh**	Optional. Enabled by default. If this feature is not enabled, you need to configure this command.
5. Enable the non-standard ORF capability for a BGP peer/peer group.	**peer** { *group-name* | *ipv6-address* } **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.
6. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—

To do...	Use the command...	Remarks
7. Enable the ORF IP prefix negotiation capability for a BGP peer/peer group.	**peer** { *group-name* | *ipv6-address* } **capability-advertise orf ip-prefix** { **both** | **receive** | **send** }	Required. Not supported by default.

Table 19 Description of the both, send, and receive parameters and the negotiation result

Local parameter	Peer parameter	Negotiation result
send	**receive**	The ORF sending capability is enabled locally and the ORF receiving capability is enabled on the peer.
	both	
receive	**send**	The ORF receiving capability is enabled locally and the ORF sending capability is enabled on the peer.
	both	
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

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
4. Configure the maximum number of equal-cost routes for load balancing.	**balance** *number*	Required. By default, load balancing is disabled.

Configuring a large scale IPv6 MBGP network

Prerequisites

Before configuring a large scale IPv6 MBGP network, configure IPv6 MBGP basic functions.

Configuring an IPv6 MBGP peer group

For easy management and configuration, organize some IPv6 MBGP peers that have the same route update policy into a group—known as a "peer group". A policy configured for a peer group applies to all the members in the group.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—

To do...	Use the command...	Remarks
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 address family view.	**ipv6-family**	—
4. Create an IPv6 BGP peer group.	**group** *ipv6-group-name* [**external** | **internal**]	Required.
5. Add a peer to the peer group.	**peer** *ipv6-address* **group** *ipv6-group-name* [**as-number** *as-number*]	Required. By default, no peer is added.
6. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
7. Enable the configured IPv6 unicast BGP peer group to create the IPv6 MBGP peer group.	**peer** *ipv6-group-name* **enable**	Required.
8. Add the IPv6 MBGP peer into the peer group.	**peer** *ipv6-address* **group** *ipv6-group-name*	Required. By default, no peer is added.

To create an IPv6 MBGP peer group, you need to 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 need to add the corresponding IPv6 BGP unicast peer to the corresponding IPv6 BGP unicast peer group.

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 needed.

To do...	Use the command...	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view	**ipv6-family multicast**	—
4. Advertise the community attribute to an IPv6 MBGP peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **advertise-community**	Required. By default, no community attribute is advertised to any peer group/peer.
5. Advertise the extended community attribute to an IPv6 MBGP peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **advertise-ext-community**	Required. By default, no extended community attribute is advertised to any peer/peer group.
6. Apply a routing policy to routes sent to an IPv6 MBGP peer/peer group.	**peer** { *ipv6-group-name* | *ipv6-address* } **route-policy** *route-policy-name* **export**	Required. Not configured by default.

You need to configure a routing policy to define the community attribute, and apply the policy to outgoing routes.

For routing policy configuration, see *Routing Policy* in the *Layer 3 – IP Routing Configuration Guide*.

Configuring an IPv6 MBGP route reflector

To guarantee connectivity between IPv6 multicast iBGP peers, you need to make them fully meshed, but it becomes unpractical when too many IPv6 multicast iBGP peers exist. Using route reflectors can solve the problem.

To do…	Use the command…	Remarks
1. Enter system view.	**system-view**	—
2. Enter BGP view.	**bgp** *as-number*	—
3. Enter IPv6 MBGP address family view.	**ipv6-family multicast**	—
4. Configure the router as a route reflector and specify an IPv6 MBGP peer/peer group as its client.	**peer** { *ipv6-group-name* | *ipv6-address* } **reflect-client**	Required. 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.

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 need to disable route reflection between clients to reduce routing costs.

If a cluster has multiple route reflectors, specify the same cluster ID for these route reflectors to avoid routing loops.

Displaying and maintaining IPv6 MBGP

To do…	Use the command…	Remarks
Display the IPv6 MBGP peer group information.	**display bgp ipv6 multicast group** [*ipv6-group-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPv6 MBGP routing information injected with the **network** command.	**display bgp ipv6 multicast network** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the IPv6 MBGP AS path information of routes.	**display bgp ipv6 multicast paths** [*as-regular-expression* | **|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPv6 MBGP peer/peer group information.	**display bgp ipv6 multicast peer** [[*ipv6-address*] **verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the prefix entries in the ORF information of the specified BGP peer.	**display bgp ipv6 multicast peer** *ipv6-address* **received ipv6-prefix** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

To do...	Use the command...	Remarks
Display IPv6 MBGP routing table information.	**display bgp ipv6 multicast routing-table** [*ipv6-address prefix-length*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPv6 MBGP routing information matching a AS path ACL.	**display bgp ipv6 multicast routing-table as-path-acl** *as-path-acl-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPv6 MBGP routing information with the specified community attribute.	**display bgp ipv6 multicast routing-table community** [*aa:nn*<1-13>] [**no-advertise** | **no-export** | **no-export-subconfed**]* [**whole-match**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display routing information matching an IPv6 MBGP community list.	**display bgp ipv6 multicast routing-table community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16> [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPv6 MBGP dampened routing information.	**display bgp ipv6 multicast routing-table dampened** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPv6 MBGP dampening parameter information.	**display bgp ipv6 multicast routing-table dampening parameter** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	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** } *regular-expression*]	Available in any view.
Display IPv6 MBGP routing flap statistics.	**display bgp ipv6 multicast routing-table flap-info** [**regular-expression** *as-regular-expression* | [**as-path-acl** *as-path-acl-number* | *ipv6-address prefix-length* [**longer-match**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]]	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** *ipv6-address* { **advertised-routes** | **received-routes** } [*network-address prefix-length* | **statistic**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPv6 multicast routing information matching an AS regular expression.	**display bgp ipv6 multicast routing-table regular-expression** *as-regular-expression*	Available in any view.
Display IPv6 MBGP routing statistics.	**display bgp ipv6 multicast routing-table statistic** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the IPv6 MBGP routing table information.	**display ipv6 multicast routing-table** [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the multicast routing information of the specified destination address.	**display ipv6 multicast routing-table** *ipv6-address prefix-length* [**longer-match**] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.

Resetting IPv6 MBGP connections

When an IPv6 MBGP routing policy is changed, you can make the new configuration effective by resetting the IPv6 MBGP connections.

To do…	Use the command…	Remarks
Reset specified IPv6 MBGP connections.	**reset bgp ipv6 multicast** { *as-number* | *ipv6-address* | **all** | **group** *ipv6-group-name* | **external** | **internal** }	Available in user view.

Clearing IPv6 MBGP information

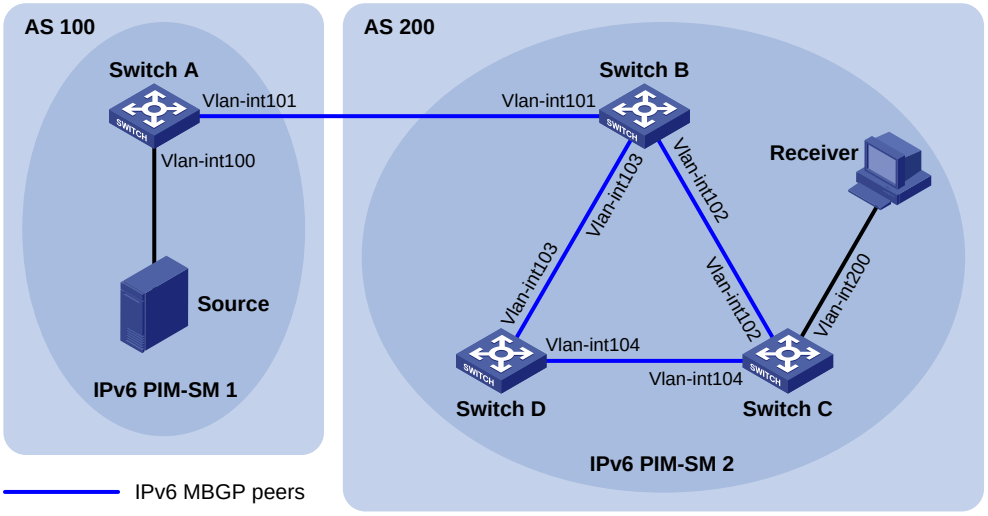
To do…	Use the command…	Remarks
Clear dampened IPv6 MBGP routing information and release suppressed routes.	**reset bgp ipv6 multicast dampening** [*ipv6-address prefix-length*]	Available in user view.
Clear IPv6 MBGP route flap statistics.	**reset bgp ipv6 multicast flap-info** [*ipv6-address/prefix-length* | **regexp** *as-path-regexp* | **as-path-acl** *as-path-acl-number*]	Available in user view.

IPv6 MBGP configuration example

Network requirements

- 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.
- Configure VLAN-interface 101 of Switch A and Switch B as the C-BSR and C-RP of the respective IPv6 PIM-SM domains.

Figure 117 Network diagram for IPv6 MBGP configuration



Device	Interface	IP address	Device	Interface	IP address
Source	-	1002::100/64	Switch C	Vlan-int200	3002::1/64
Switch A	Vlan-int100	1002::1/64		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			

Procedure

1. Configure IPv6 addresses for interfaces as shown in Figure 117. Detailed configuration steps are omitted here.
2. Configure OSPFv3. Detailed configuration steps are omitted here.
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. Configure the position of C-BSR and C-RP.

Configure the position of C-BSR and C-RP on Switch A.

```
[SwitchA] pim ipv6
[SwitchA-pim6] c-bsr 1001::1
[SwitchA-pim6] c-rp 1001::1
[SwitchA-pim6] quit
```

Configure the position of C-BSR and C-RP on Switch B.

```
[SwitchB] pim ipv6
[SwitchB-pim6] c-bsr 1001::2
[SwitchB-pim6] c-rp 1001::2
[SwitchB-pim6] quit
```

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] ipv6
[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] ipv6
[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 **display bgp ipv6 multicast peer** 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 A-Series 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

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.
Italic	*Italic* 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.
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.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index