HP MSR2000/3000/4000 Router Series

IP Multicast

Configuration Guide (V7)

Part number: 5998-3993

Software version: CMW710-R0007P02

Document version: 6PW100-20130927

Legal and notice information

The information contained herein is subject to change without notice.

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

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

Contents

Multicast overview

Introduction to multicast

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

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

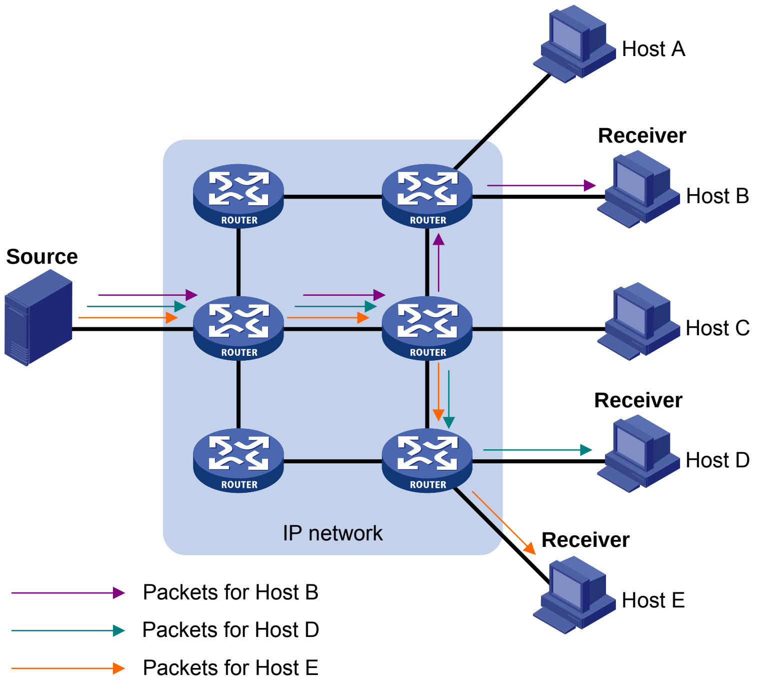
Information transmission techniques

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

Unicast

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

Figure 1 Unicast transmission



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

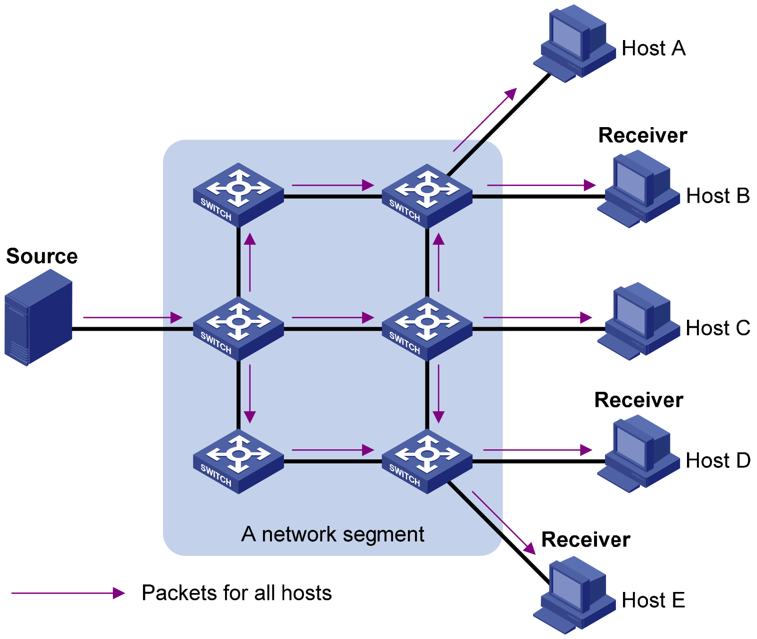
In unicast transmission, the traffic transmitted over the network is proportional to the number of hosts that need the information. If a large number of hosts need the information, the information source must send a separate copy of the same information to each of these hosts. Sending many copies can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

Unicast is not suitable for batch transmission of information.

Broadcast

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

Figure 2 Broadcast transmission



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

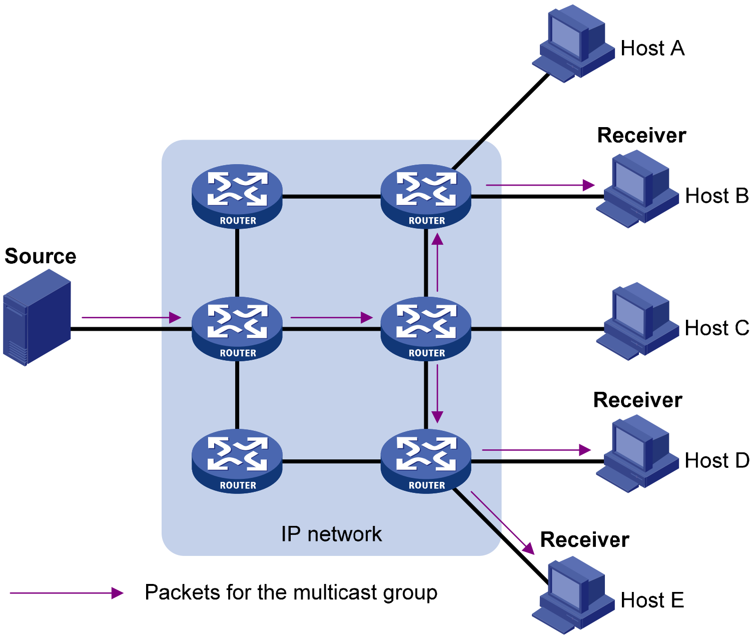
Broadcast is not as efficient as multicast for sending data to groups of hosts.

Multicast

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

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

Figure 3 Multicast transmission



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

To summarize, multicast has the following advantages:

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

Multicast features

- A multicast group is a multicast receiver set identified by an IP multicast address. Hosts must join a multicast group to become members of the multicast group before they 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.
- The group memberships are dynamic. Hosts can join or leave multicast groups at any time. Multicast groups are not subject to geographic restrictions.
- Routers or Layer 3 switches that support Layer 3 multicast are called "multicast routers" or "Layer 3 multicast devices." In addition to providing the multicast routing function, a multicast router can also manage multicast group memberships on stub subnets with attached group members. A multicast router itself can be a multicast group member.

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

Table 1 Comparing TV program transmission and multicast transmission

TV program 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 on the channel.	The receiver starts to receive the multicast data that the source is sending to the multicast group.
The user turns off the TV set or tunes to another channel.	The receiver leaves the multicast group or joins another group.

Common notations in multicast

The following notations are commonly used in multicast transmission:

- **(*, G)**—Rendezvous point tree (RPT), or a multicast packet that any multicast source sends to multicast group G. The asterisk (*) represents any multicast source, and "G" represents a specific multicast group.
- **(S, G)**—Shortest path tree (SPT), or a multicast packet that multicast source "S" sends to multicast group "G." "S" represents a specific multicast source, and "G" represents a specific multicast group.

For more information about the concepts RPT and SPT, see "Configuring PIM" and "Configuring IPv6 PIM."

Multicast benefits and applications

Multicast benefits

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

Multicast applications

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

Multicast models

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

ASM model

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

SFM model

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

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

SSM model

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

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

Multicast architecture

IP multicast addresses the following issues:

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

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

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

Multicast addresses

IP multicast addresses

- IPv4 multicast addresses:

  IANA assigns the Class D address block (224.0.0.0 to 239.255.255.255) to IPv4 multicast.

  Table 2 Class D IP address blocks and description

Address block	Description
224.0.0.0 to 224.0.0.255	Reserved permanent group addresses. The IP address 224.0.0.0 is reserved. Other IP addresses can be used by routing protocols and for topology searching, and protocol maintenance. 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. You can reuse them in domains administered by different organizations without causing conflicts. For more information, see RFC 2365.

NOTE:

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

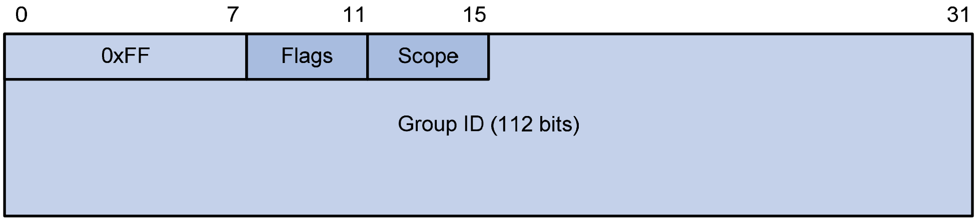
Table 3 Some reserved multicast addresses

Address	Description
224.0.0.1	All systems on this subnet, including hosts and routers.
224.0.0.2	All multicast routers on this subnet.
224.0.0.3	Unassigned.
224.0.0.4	DVMRP routers.
224.0.0.5	OSPF routers.
224.0.0.6	OSPF designated routers and backup designated routers.
224.0.0.7	Shared Tree (ST) routers.
224.0.0.8	ST hosts.
224.0.0.9	RIPv2 routers.
224.0.0.11	Mobile agents.
224.0.0.12	DHCP server/relay agent.
224.0.0.13	All Protocol Independent Multicast (PIM) routers.

Address	Description
224.0.0.14	RSVP encapsulation.
224.0.0.15	All Core-Based Tree (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 address format



The following describes the fields of an IPv6 multicast address:

- **0xFF**—The most significant eight bits are 11111111. This address is an IPv6 multicast address.
- **Flags**—The Flags field contains four bits.

Figure 5 Flags field format

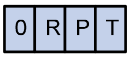


Table 4 Flags field description

Bit	Description
0	Reserved, set to 0.
R	• When set to 0, this address is an IPv6 multicast address without an embedded RP address. • When set to 1, 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, this address is an IPv6 multicast address not based on a unicast prefix. • When set to 1, 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, this address is an IPv6 multicast address permanently-assigned by IANA. • When set to 1, this address is a transient, or dynamically assigned IPv6 multicast address.

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

Table 5 Values of the Scope field

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

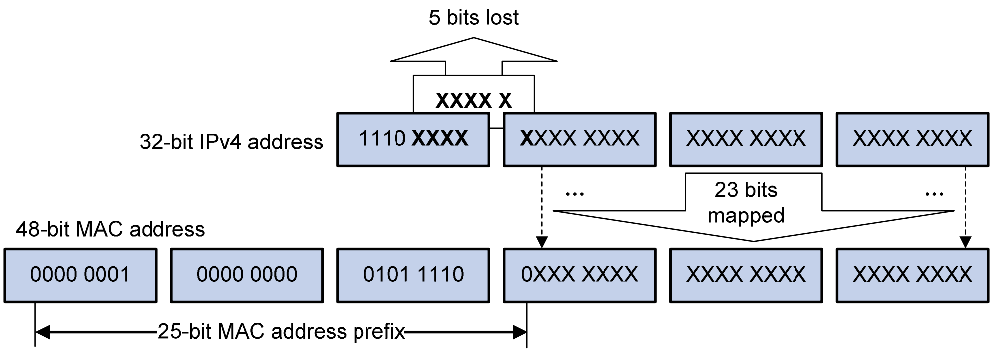
- **Group ID**—The Group ID field contains 112 bits. It uniquely identifies an IPv6 multicast group in the scope that the Scope field defines.

Ethernet multicast MAC addresses

- IPv4 multicast MAC addresses:

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

  Figure 6 IPv4-to-MAC address mapping

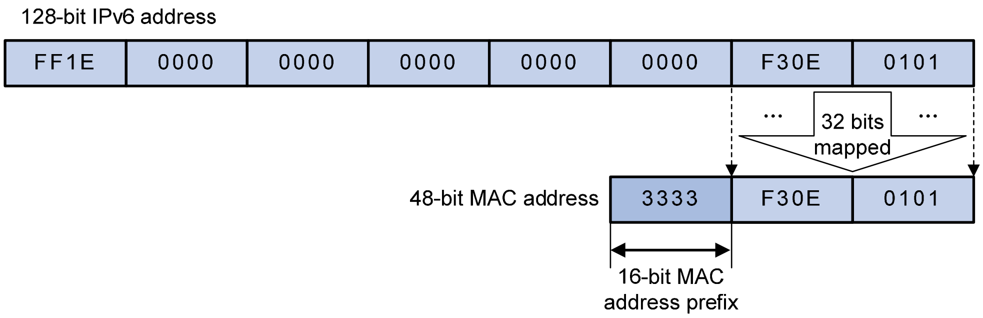


  The most significant four bits of a multicast IPv4 address are 1110. Only 23 bits of the remaining 28 bits are mapped to a MAC address, so five bits of the multicast IPv4 address are lost. As a result, 32 multicast IPv4 addresses map to the same IPv4 multicast MAC address. Therefore, a device might receive some unwanted multicast data at Layer 2 processing, which needs to be filtered by the upper layer.

- IPv6 multicast MAC addresses:

  As defined by IANA, the most significant 16 bits of an IPv6 multicast MAC address are 0x3333 as its address prefix. The least significant 32 bits are the least significant 32 bits of a multicast IPv6 address and are mapped to the remaining IPv6 multicast MAC address, so the problem of duplicate IPv6-to-MAC address mapping also arises like IPv4-to-MAC address mapping.

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



IMPORTANT:

Because of the duplicate mapping from multicast IP address to multicast MAC address, the device might inadvertently send multicast protocol packets as multicast data in Layer 2 forwarding. To avoid this, do not use the IP multicast addresses that are mapped to multicast MAC addresses 0100-5E00-00xx and 3333-0000-00xx (where "x" specifies any hexadecimal number from 0 to F).

Multicast protocols

Multicast protocols include the following categories:

- Layer 3 and Layer 2 multicast protocols:
  - Layer 3 multicast refers to IP multicast working at the network layer.

    Layer 3 multicast protocols—IGMP, MLD, PIM, IPv6 PIM, MSDP, MBGP, and IPv6 MBGP.
  - Layer 2 multicast refers to IP multicast working at the data link layer.

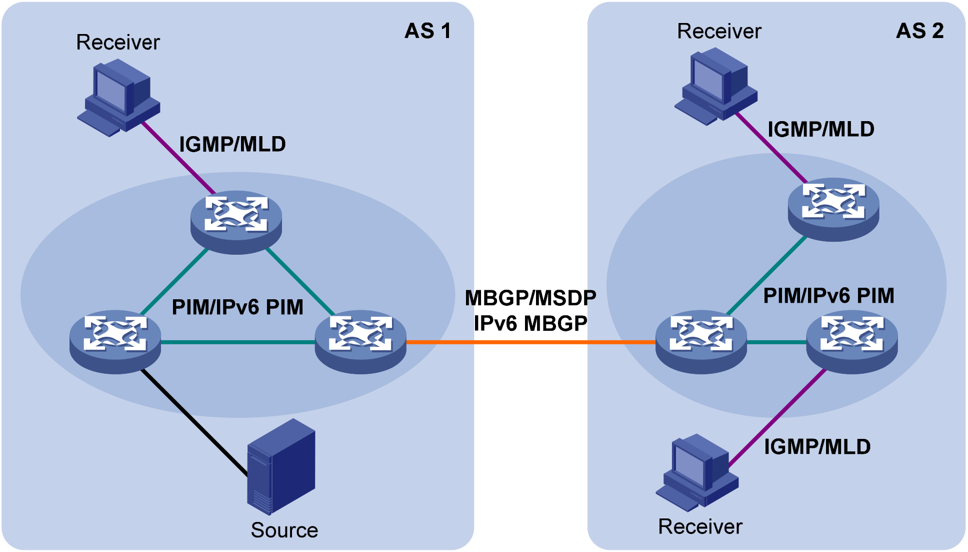
    Layer 2 multicast protocols—IGMP snooping, MLD snooping, PIM snooping, IPv6 PIM snooping, multicast VLAN, and IPv6 multicast VLAN.
- IPv4 and IPv6 multicast protocols:
  - **For IPv4 networks**—IGMP snooping, PIM snooping, multicast VLAN, IGMP, PIM, MSDP, and MBGP.
  - **For IPv6 networks**—MLD snooping, IPv6 PIM snooping, IPv6 multicast VLAN, MLD, IPv6 PIM, and IPv6 MBGP.

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

Layer 3 multicast protocols

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

Figure 8 Positions of Layer 3 multicast protocols



- Multicast group management protocols:

  Typically, the Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD) protocol is used between hosts and Layer 3 multicast devices that directly connect to the hosts to define how to establish and maintain their multicast group memberships.

- Multicast routing protocols:

  A multicast routing protocol runs on Layer 3 multicast devices to establish and maintain multicast routes and correctly and efficiently forward multicast packets. Multicast routes constitute loop-free data transmission paths (also known as multicast distribution trees) from a data source to multiple receivers.

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

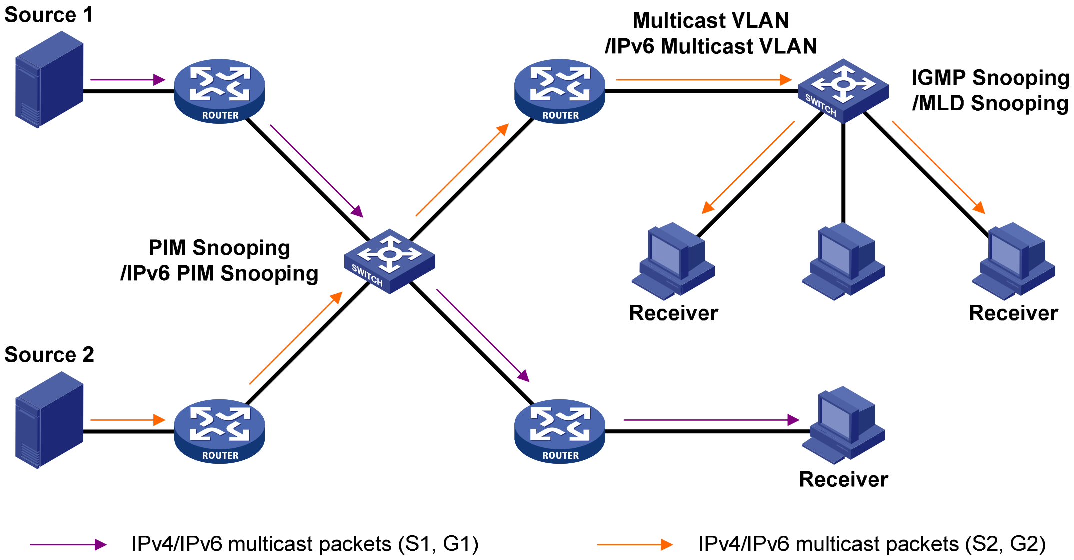
  - An intra-domain multicast routing protocol discovers multicast sources and builds multicast distribution trees within an AS to deliver multicast data to receivers. Among a variety of mature intra-domain multicast routing protocols, PIM is most widely used. Based on the forwarding mechanism, PIM has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

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

Layer 2 multicast protocols

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

Figure 9 Positions of Layer 2 multicast protocols



- IGMP snooping and MLD snooping:

  IGMP snooping and MLD snooping are multicast constraining mechanisms that run on Layer 2 devices. They generate Layer 2 multicast forwarding tables by listening to IGMP or MLD messages exchanged between the hosts and Layer 3 multicast devices, and manage and control multicast data forwarding on demand in Layer 2 networks.
- PIM snooping and IPv6 PIM snooping:

  PIM snooping and IPv6 PIM snooping run on Layer 2 devices. They work with IGMP snooping or MLD snooping to analyze received PIM messages, and adds the ports that are interested in specific multicast data to a PIM snooping routing entry or IPv6 PIM snooping routing entry. In this way, multicast data can be forwarded to only the ports that are interested in the data.
- Multicast VLAN and IPv6 multicast VLAN:

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

Multicast packet forwarding mechanism

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

- To ensure multicast packet transmission in the network, unicast routing tables, routing tables for multicast (for example, the MBGP routing table), and static multicast routes must be used as guidance for multicast forwarding.
- To process the same multicast information from different peers received on different interfaces of the same device, every multicast packet undergoes a reverse path forwarding (RPF) check on the

incoming interface. The RPF check result determines whether the packet will be forwarded or discarded. The RPF check mechanism is the basis for most multicast routing protocols to implement multicast forwarding.

For more information about the RPF mechanism, see "Configuring multicast routing and forwarding" and "Configuring IPv6 multicast routing and forwarding."

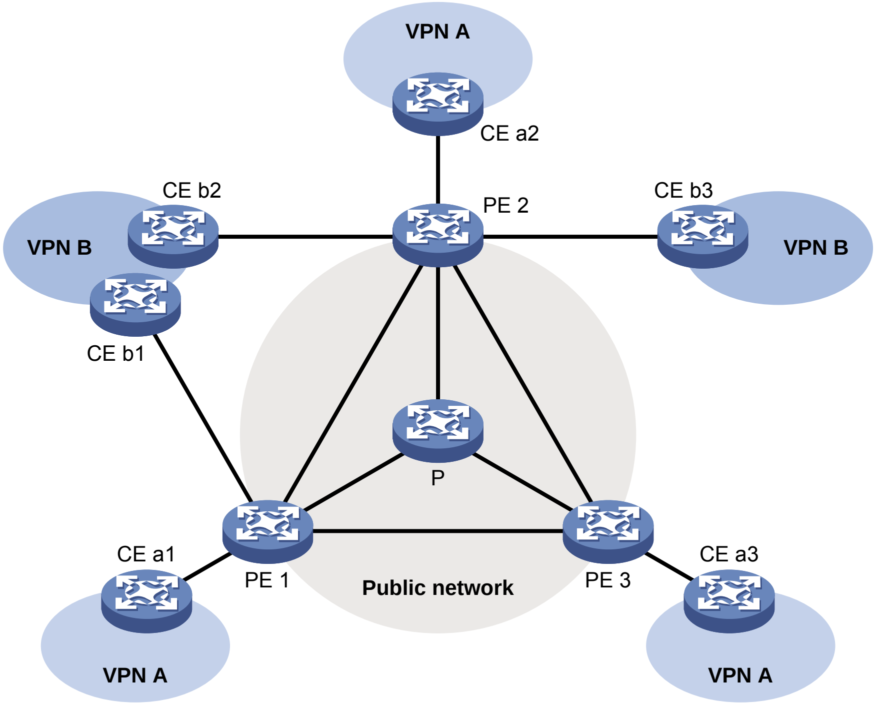
Multicast support for VPNs

Multicast support for VPNs refers to multicast applied in VPNs.

Introduction to VPN instances

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

Figure 10 VPN networking diagram



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

Multicast application in VPNs

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

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

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

Configuring IGMP snooping

Feature and hardware compatibility

IGMP snooping is available only on the MSR series routers with Ethernet Layer 2 switching interface modules. For information about the Ethernet Layer 2 switching interface modules, see *HP MSR Router Series Interface Module Guide*.

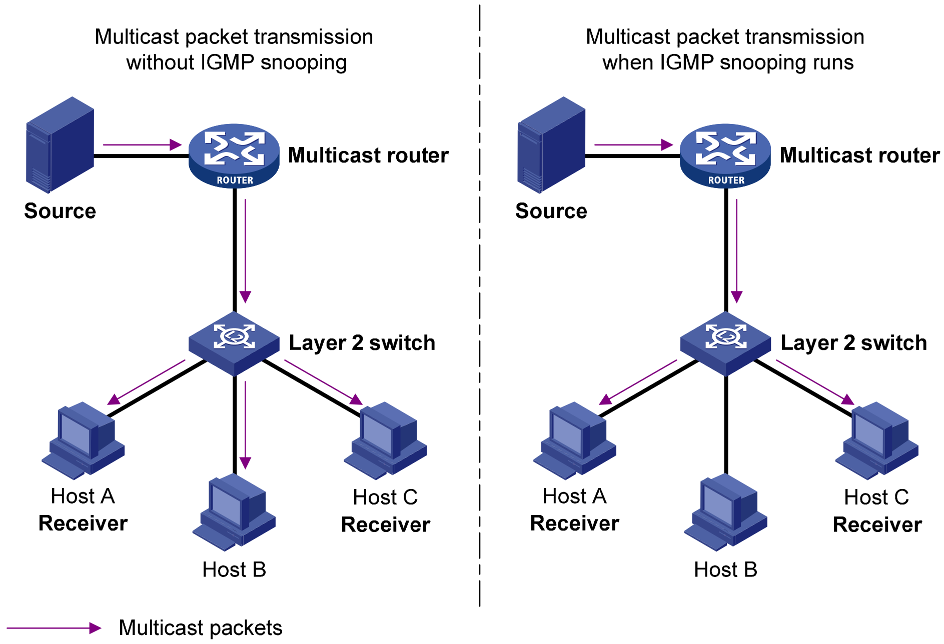
The term "switch" in this document refers to the MSR series routers with Ethernet Layer 2 switching interface modules.

Overview

IGMP snooping runs on a Layer 2 switch as a multicast constraining mechanism to improve multicast forwarding efficiency. It creates Layer 2 multicast forwarding entries from IGMP packets that are exchanged between the hosts and the router.

As shown in Figure 11, when IGMP snooping is not enabled, the Layer 2 switch floods multicast packets to all hosts. When IGMP snooping is enabled, the Layer 2 switch forwards multicast packets of known multicast groups to only the receivers.

Figure 11 Multicast packet transmission without and with IGMP snooping

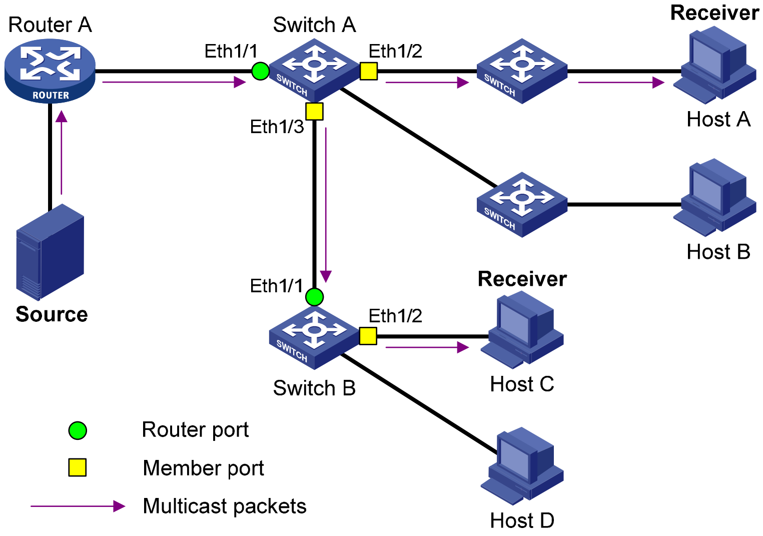


Basic IGMP snooping concepts

IGMP snooping related ports

As shown in Figure 12, IGMP snooping runs on Switch A and Switch B, and Host A and Host C are receivers in a multicast group.

Figure 12 IGMP snooping related ports



The following describes the ports involved in IGMP snooping:

- **Router port**—Layer 3 multicast device-side port. Layer 3 multicast devices include designated routers (DRs) and IGMP queriers. In Figure 12, Ethernet 1/1 of Switch A and Ethernet 1/1 of Switch B are the router ports. A switch records all its router ports in a router port list.

  Do not confuse the "router port" in IGMP snooping with the "routed interface" commonly known as the "Layer 3 interface." The router port in IGMP snooping is a Layer 2 interface.
- **Member port**—Multicast receiver-side port. In Figure 12, Ethernet 1/2 and Ethernet 1/3 of Switch A and Ethernet 1/2 of Switch B are the member ports. A switch records all its member ports in the IGMP snooping forwarding table.

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

NOTE:

When IGMP snooping is enabled, all ports that receive PIM hello messages or IGMP general queries with the source addresses other than 0.0.0.0 are considered dynamic router ports. For more information about PIM hello messages, see "Configuring PIM."

Aging timers for dynamic ports in IGMP snooping

Timer	Description	Message received before the timer expires	Action after the timer expires
Dynamic router port aging timer.	When a port recieves an IGMP general query with the source address other than 0.0.0.0 or PIM hello message, the switch starts or resets an aging timer for it. When the timer expires, the dynamic router port ages out.	IGMP general query with the source address other than 0.0.0.0 or PIM hello message.	The switch removes the port from its router port list.
Dynamic member port aging timer.	When a port dynamically joins a multicast group, the switch starts or resets an aging timer for the port. When the timer expires, the dynamic member port ages out.	IGMP membership report.	The switch removes the port from the IGMP snooping forwarding table.

NOTE:

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

How IGMP snooping works

The ports in this section are dynamic ports. For information about how to configure and remove static ports, see "Configuring static ports."

IGMP messages are general query, IGMP report, and leave message. An IGMP snooping-enabled switch performs differently depending on the message.

General query

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

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

- If the port that received the query is a dynamic router port in the router port list, the switch restarts the aging timer for the port.
- If the port that received the query does not exist in the router port list, the switch adds the port to the router port list, and starts an aging timer for the port.

IGMP report

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

- Responds to queries if the host is a multicast group member.
- Applies for a multicast group membership.

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

- If no forwarding entry matches the group address, the switch creates a forwarding entry for the group, adds the receiving port as a dynamic member port to the forwarding entry, and starts an aging timer for the port.

- If a forwarding entry matches the group address, but the receiving port is not in the forwarding entry for the group, the switch adds the port as a dynamic member port to the forwarding entry, and starts an aging timer for the port.
- If a forwarding entry matches the group address and the receiving port is in the forwarding entry for the group, the switch restarts the aging timer for the port.

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

A switch does not forward an IGMP report through a non-router port. If the switch forwards a report message through a member port, the IGMP report suppression mechanism causes all attached hosts that monitor the reported multicast address to suppress their own reports. In this case, the switch cannot determine whether the reported multicast group still has active members attached to that port. For more information about the IGMP report suppression mechanism, see "Configuring IGMP."

Leave message

An IGMPv1 host silently leaves a multicast group, and the switch is not notified of the leaving. However, because the host stops sending IGMP reports as soon as it leaves the multicast group, the switch removes the port that connects to the host from the forwarding entry for the multicast group when the aging timer for the port expires.

An IGMPv2 or IGMPv3 host sends an IGMP leave message to the multicast router when it leaves a multicast group.

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

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

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

- If the port (assuming that it is a dynamic member port) receives an IGMP report in response to the group-specific query before its aging timer expires, it means that some host attached to the port is receiving or expecting to receive multicast data for the multicast group. The switch restarts the aging timer for the port.
- If the port receives no IGMP report in response to the group-specific query before its aging timer expires, it means that no hosts attached to the port are still listening to that group address. The switch removes the port from the forwarding entry for the multicast group after the aging timer for the port expires.

Protocols and standards

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

IGMP snooping configuration task list

Task at a glance
Configuring basic IGMP snooping functions • (Required.) Enabling IGMP snooping • (Optional.) Specifying the IGMP snooping version • (Optional.) Setting the maximum number of IGMP snooping forwarding entries • (Optional.) Configuring parameters for IGMP queries and responses
Configuring IGMP snooping port functions • (Optional.) Setting aging timers for dynamic ports • (Optional.) Configuring static ports • (Optional.) Enabling IGMP snooping fast-leave processing
Configuring IGMP snooping policies • (Optional.) Configuring a multicast group filter • (Optional.) Setting the maximum number of multicast groups on a port • (Optional.) Enabling the multicast group replacement function

Configuring basic IGMP snooping functions

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

- Configure the corresponding VLANs.
- Determine the IGMP snooping version.
- Determine the IGMP last-member query interval.
- Determine the maximum response delay for IGMP general queries.

Enabling IGMP snooping

When you enable IGMP snooping, follow these guidelines:

- You must enable IGMP snooping globally before you enable it for a VLAN.
- IGMP snooping for a VLAN works only on the member ports in that VLAN.

You can enable IGMP snooping for a VLAN in IGMP-snooping view, or for a VLAN in VLAN view. These configurations have the same priority level.

To enable IGMP snooping for a VLAN in IGMP-snooping view:

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

Step	Command	Remarks
2. Enable IGMP snooping globally and enter IGMP-snooping view.	**igmp-snooping**	By default, IGMP snooping is disabled.
3. Return to system view.	**quit**	N/A
4. Enable IGMP snooping for specified VLANs.	**enable vlan** *vlan-list*	By default, IGMP snooping is disabled for a VLAN.

To enable IGMP snooping for a VLAN in VLAN view:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable IGMP snooping globally and enter IGMP-snooping view.	**igmp-snooping**	By default, IGMP snooping is disabled.
3. Return to system view.	**quit**	N/A
4. Enter VLAN view.	**vlan** *vlan-id*	N/A
5. Enable IGMP snooping for the VLAN.	**igmp-snooping enable**	By default, IGMP snooping is disabled for a VLAN.

Specifying the IGMP snooping version

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

- IGMPv2 snooping can process IGMPv1 and IGMPv2 messages, but it floods IGMPv3 messages in the VLAN instead of processing them.
- IGMPv3 snooping can process IGMPv1, IGMPv2, and IGMPv3 messages.

If you change IGMPv3 snooping to IGMPv2 snooping, the device does the following:

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

For more information about static IGMP snooping forwarding entries, see "Configuring static ports."

You can specify the IGMP snooping version for a VLAN in IGMP-snooping view, or for a VLAN in VLAN view. These configurations have the same priority level.

To specify the IGMP snooping version for a VLAN in IGMP-snooping view:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable IGMP snooping globally and enter IGMP-snooping view.	**igmp-snooping**	N/A
3. Specify the IGMP snooping version for the specified VLANs	**version** *version-number* **vlan** *vlan-list*	The default setting is IGMPv2 snooping.

To specify the IGMP snooping version for a VLAN in VLAN view:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter VLAN view.	**vlan** *vlan-id*	N/A
3.	Specify the version of IGMP snooping.	**igmp-snooping version** *version-number*	The default setting is IGMPv2 snooping.

Setting the maximum number of IGMP snooping forwarding entries

You can modify the maximum number of IGMP snooping forwarding entries. When the number of forwarding entries on the device reaches the upper limit, the device does not automatically remove any existing entries or create new entries until some entries time out or are removed. In this case, HP recommends that you manually remove the excessive entries.

To set the maximum number of IGMP snooping forwarding entries:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter IGMP-snooping view.	**igmp-snooping**	N/A
3.	Set the maximum number of IGMP snooping forwarding entries.	**entry-limit** *limit*	The default setting is 4294967295.

Configuring parameters for IGMP queries and responses

When a multicast listening host receives an IGMP query (general query or group-specific query), it starts a delay 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 advertised in the IGMP query message. When the timer value decreases to 0, the host sends an IGMP report to the multicast group.

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

- The maximum response time for IGMP general queries is set by the **max-response-time** command.
- The maximum response time for IGMP group-specific queries is the same as the IGMP last-member query interval, which is set by the **last-member-query-interval** command.

You can configure parameters for IGMP queries and responses either for the current VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. If the two configurations are made in both VLAN view and IGMP-snooping view, the configuration made in VLAN view takes priority.

Configuring parameters for IGMP queries and responses globally

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

Step		Command	Remarks
2.	Enter IGMP-snooping view.	**igmp-snooping**	N/A
3.	Set the maximum response time for IGMP general queries.	**max-response-time** *interval*	The default setting is 10 seconds.
4.	Set the IGMP last-member query interval.	**last-member-query-interval** *interval*	The default setting is 1 second.

Configuring parameters for IGMP queries and responses in a VLAN

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter VLAN view.	**vlan** *vlan-id*	N/A
3.	Set the maximum response time for IGMP general queries in the VLAN.	**igmp-snooping max-response-time** *interval*	The default setting is 10 seconds.
4.	Set the IGMP last-member query interval.	**igmp-snooping last-member-query-interval** *interval*	The default setting is 1 second.

Configuring IGMP snooping port functions

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

- Enable IGMP snooping for the VLAN.
- Determine the aging timer for dynamic router ports.
- Determine the aging timer for dynamic member ports.
- Determine the addresses of the multicast group and multicast source.

Setting aging timers for dynamic ports

When you set aging timers for dynamic ports, follow these guidelines:

- If the memberships of multicast groups frequently change, you can set a relatively small value for the aging timer of the dynamic member ports. If the memberships of multicast groups rarely change, you can set a relatively large value.
- If a dynamic router port receives a PIMv2 hello message, the aging timer for the port is the timer in the hello message rather than the timer configured by using the **router-aging-time** command or the **igmp-snooping router-aging-time** command.
- You can set the aging timers for dynamic ports either for the current VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. If the configurations are made in both VLAN view and IGMP-snooping view, the configuration made in VLAN view takes priority.

Setting the aging timers for dynamic ports globally

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

Step		Command	Remarks
2.	Enter IGMP-snooping view.	**igmp-snooping**	N/A
3.	Set the aging timer for dynamic router ports globally.	**router-aging-time** *interval*	The default setting is 260 seconds.
4.	Set the global aging timer for dynamic member ports globally.	**host-aging-time** *interval*	The default setting is 260 seconds.

Setting the aging timers for the dynamic ports in a VLAN

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter VLAN view.	**vlan** *vlan-id*	N/A
3.	Set the aging timer for the dynamic router ports in the VLAN.	**igmp-snooping router-aging-time** *interval*	The default setting is 260 seconds.
4.	Set the aging timer for the dynamic member ports in the VLAN.	**igmp-snooping host-aging-time** *interval*	The default setting is 260 seconds.

Configuring static ports

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

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

When you configure static ports, follow these guidelines:

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

To configure static ports:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure the port as a static member port.	**igmp-snooping static-group** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	By default, a port is not a static member port.
4.	Configure the port as a static router port.	**igmp-snooping static-router-port vlan** *vlan-id*	By default, a port is not a static router port.

Enabling IGMP snooping fast-leave processing

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

When you enable the IGMP snooping fast-leave processing feature, follow these guidelines:

- In a VLAN, you can enable IGMP snooping fast-leave processing on ports that have only one receiver host attached. If a port has multiple hosts attached, do not enable IGMP snooping fast-leave processing on this port. Otherwise, other receiver hosts attached to this port in the same multicast group cannot receive the multicast data destined to this group.
- You can enable IGMP snooping fast-leave processing either for the current port in proper interface view or globally for all ports in IGMP-snooping view. If the configurations are made both in interface view and IGMP-snooping view, the configuration made in interface view takes priority.

Enabling IGMP snooping fast-leave processing globally

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter IGMP-snooping view.	**igmp-snooping**	N/A
3. Enable IGMP snooping fast-leave processing globally.	**fast-leave** [**vlan** *vlan-list*]	By default, fast-leave processing is disabled.

Enabling IGMP snooping fast-leave processing on a port

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable IGMP snooping fast-leave processing on the port.	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	By default, fast-leave processing is disabled.

Configuring IGMP snooping policies

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

- Enable IGMP snooping for the VLAN.
- Determine the ACL used as the multicast group filter.
- Determine the maximum number of multicast groups that a port can join.

Configuring a multicast group filter

When you configure a multicast group filter, follow these guidelines:

- This configuration takes effect on the multicast groups that a port dynamically joins. If you configure the port as a static member port for a multicast group, this configuration does not take effect on the multicast group.
- You can configure a multicast filter either for the current port in proper interface view or globally for all ports in IGMP-snooping view. If the configurations are made in both interface view and IGMP-snooping view, the configuration made in interface view takes priority.

Configuring a multicast group filter globally

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

Configuring a multicast group filter on a port

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure a multicast group filter on a port.	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	By default, no multicast group filter is configured on a port. The hosts on this port can join any valid multicast group.

Setting the maximum number of multicast groups on a port

You can set the maximum number of multicast groups on a port to regulate the port traffic.

When you set the maximum number of multicast groups on a port, follow these guidelines:

- This configuration takes effect on the multicast groups that a port dynamically joins. If you configure the port as a static member port for a multicast group, this configuration does not take effect on the multicast group.
- If the number of multicast groups on a port exceeds the limit, the system removes all the forwarding entries related to that port from the IGMP snooping forwarding table. The receiver hosts attached to that port can join multicast groups again before the number of multicast groups on the port reaches the limit.

To set the maximum number of multicast groups on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Set the maximum number of multicast groups on a port.	**igmp-snooping group-limit** *limit* [**vlan** *vlan-list*]	The default setting is 4294967295.

Enabling the multicast group replacement function

When the number of multicast groups on a switch or a port exceeds the limit:

- If the multicast group replacement is enabled, the switch or the port replaces an existing multicast group with a newly joined multicast group.
- If the multicast group replacement is disabled, the switch or the port discards IGMP reports that are used for joining a new multicast group.

In some specific applications, such as channel switching, a newly joined multicast group must automatically replace an existing multicast group. In this case, the function of multicast group replacement must also be enabled so a user can switch from the current multicast group to a new group.

When you enable the multicast group replacement function, follow these guidelines:

- This configuration takes effect on the multicast groups that a port dynamically joins. If you configure the port as a static member port for a multicast group, this configuration does not take effect on the multicast group.
- You can enable the multicast group replacement function either for the current port in proper interface view or globally for all ports in IGMP-snooping view. If the configurations are made in both interface view and IGMP-snooping view, the configuration made in interface view takes priority.

To enable the multicast group replacement function globally:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter IGMP-snooping view.	**igmp-snooping**	N/A
3.	Enable the multicast group replacement function globally.	**overflow-replace** [**vlan** *vlan-list*]	By default, the multicast group replacement function is disabled.

To enable the multicast group replacement function on a port:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3.	Enable multicast group replacement function on a port.	**igmp-snooping overflow-replace** [**vlan** *vlan-list*]	By default, the multicast group replacement function is disabled.

Displaying and maintaining IGMP snooping

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display IGMP snooping status.	**display igmp-snooping** [**global** | **vlan** *vlan-id*]

Task	Command
Display information about dynamic IGMP snooping forwarding entries (MSR2000/MSR3000).	**display igmp-snooping group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**]
Display information about dynamic IGMP snooping forwarding entries (MSR4000).	**display igmp-snooping group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
Display information about static IGMP snooping forwarding entries (MSR2000/MSR3000).	**display igmp-snooping static-group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**]
Display information about static IGMP snooping forwarding entries (MSR4000).	**display igmp-snooping static-group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]
Display information about dynamic router ports (MSR2000/MSR3000).	**display igmp-snooping router-port** [**vlan** *vlan-id*]
Display information about dynamic router ports (MSR4000).	**display igmp-snooping router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
Display information about static router ports (MSR2000/MSR3000).	**display igmp-snooping static-router-port** [**vlan** *vlan-id*]
Display information about static router ports (MSR4000).	**display igmp-snooping static-router-port** [**vlan** *vlan-id*] [**slot** *slot-number*]
Display statistics for the IGMP messages learned by IGMP snooping.	**display igmp-snooping statistics**
Display information about Layer 2 IP multicast groups (MSR2000/MSR3000).	**display l2-multicast ip** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*]
Display information about Layer 2 IP multicast groups (MSR4000).	**display l2-multicast ip** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
Display information about Layer 2 IP multicast group entries (MSR2000/MSR3000).	**display l2-multicast ip forwarding** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*]
Display information about Layer 2 IP multicast group entries (MSR4000).	**display l2-multicast ip forwarding** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]
Display information about Layer 2 MAC multicast groups (MSR2000/MSR3000).	**display l2-multicast mac** [*mac-address*] [**vlan** *vlan-id*]
Display information about Layer 2 MAC multicast groups (MSR4000).	**display l2-multicast mac** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
Display information about Layer 2 MAC multicast group entries (MSR2000/MSR3000).	**display l2-multicast mac forwarding** [*mac-address*] [**vlan** *vlan-id*]
Display information about Layer 2 MAC multicast group entries (MSR4000).	**display l2-multicast mac forwarding** [*mac-address*] [**vlan** *vlan-id*] [**slot** *slot-number*]
Remove the dynamic IGMP snooping forwarding entries for the specified multicast groups.	**reset igmp-snooping group** { *group-address* [*source-address*] | **all** } [**vlan** *vlan-id*]
Remove dynamic router ports.	**reset igmp-snooping router-port** { **all** | **vlan** *vlan-id* }
Clear statistics for the IGMP messages learned by IGMP snooping.	**reset igmp-snooping statistics**

Static port configuration example

Network requirements

As shown in Figure 13, Router A runs IGMPv2 and serves as the IGMP querier. Switch A, Switch B, and Switch C run IGMPv2 snooping.

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

Suppose the 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 data flows to the receivers attached to Switch C only along the path of Switch A—Switch B—Switch C.

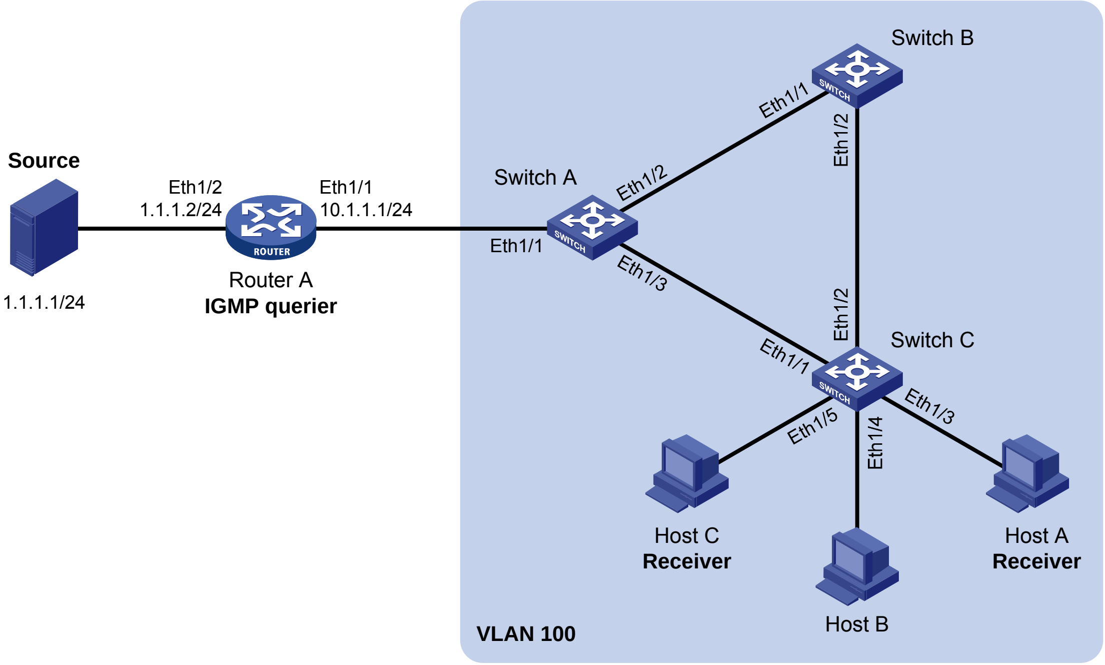
Configure Ethernet 1/3 on Switch A as a static router port, so that multicast data can flow to the receivers nearly uninterruptedly along the path of Switch A—Switch C when the path of Switch A—Switch B—Switch C is blocked.

NOTE:

If no static router port is configured, when the path of Switch A—Switch B—Switch C is 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, so multicast delivery is interrupted during this process.

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

Figure 13 Network diagram



Configuration procedure

1. Assign an IP address and subnet mask to each interface as shown in Figure 13. (Details not shown.)
2. On Router A, enable IP multicast routing globally, enable IGMP on Ethernet 1/1, and enable PIM-DM on each interface.

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] igmp enable
[RouterA-Ethernet1/1] pim dm
[RouterA-Ethernet1/1] quit
[RouterA] interface ethernet 1/2
[RouterA-Ethernet1/2] pim dm
[RouterA-Ethernet1/2] quit
```

3. Configure Switch A:

# Enable IGMP snooping globally.

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

# Create VLAN 100, assign Ethernet 1/1 through Ethernet 1/3 to the VLAN, and enable IGMP snooping for the VLAN.

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

# Configure Ethernet 1/3 as a static router port.

```
[SwitchA] interface ethernet 1/3
[SwitchA-Ethernet1/3] igmp-snooping static-router-port vlan 100
[SwitchA-Ethernet1/3] quit
```

4. Configure Switch B:

# Enable IGMP snooping globally.

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

# Create VLAN 100, assign Ethernet 1/1 and Ethernet 1/2 to the VLAN, and enable IGMP snooping for the VLAN.

```
[SwitchB] vlan 100
[SwitchB-vlan100] port ethernet 1/1 ethernet 1/2
[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 Ethernet 1/1 through Ethernet 1/5 to the VLAN, and enable IGMP snooping for the VLAN.

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

# Configure Ethernet 1/3 and Ethernet 1/5 as static member ports for multicast group 224.1.1.1.

```
[SwitchC] interface Ethernet 1/3
[SwitchC-Ethernet1/3] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-Ethernet1/3] quit
[SwitchC] interface Ethernet 1/5
[SwitchC-Ethernet1/5] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-Ethernet1/5] quit
```

Verifying the configuration

# Display information about the static router ports in VLAN 100 on Switch A.

```
[SwitchA] display igmp-snooping static-router-port vlan 100
VLAN 100:
  Router slots (1 in total):
    1
  Router ports (1 in total):
    1
    Eth1/3
```

The output shows that Ethernet 1/3 on Switch A has become a static router port.

# Display information about the static IGMP snooping forwarding entries in VLAN 100 on Switch C.

```
[SwitchC] display igmp-snooping static-group vlan 100
Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Host slots (1 in total):
      1
    Host ports (2 in total):
      Eth1/3
      Eth1/5
```

The output shows that Ethernet 1/3 and Ethernet 1/5 on Switch C have become static member ports of the multicast group 224.1.1.1.

Troubleshooting IGMP snooping

Layer 2 multicast forwarding cannot function

Symptom

Layer 2 multicast forwarding cannot function on the switch.

Analysis

IGMP snooping is not enabled.

Solution

1. Use the **display igmp-snooping** command to display IGMP snooping status.
2. If IGMP snooping is not enabled, use the **igmp-snooping** command in system view to enable IGMP snooping globally, and then use the **igmp-snooping enable** command in VLAN view to enable IGMP snooping for the VLAN.
3. If IGMP snooping is enabled globally but not enabled for the VLAN, use the **igmp-snooping enable** command in VLAN view to enable IGMP snooping for the VLAN.

Configuring multicast routing and forwarding

Overview

The following tables are involved in multicast routing and forwarding:

- Multicast routing table of each multicast routing protocol, such as the PIM routing table.
- General multicast routing table that summarizes multicast routing information generated by different multicast routing protocols. The multicast routing information from multicast sources to multicast groups are stored in a set of (S, G) routing entries.
- Multicast forwarding table that guides multicast forwarding. The optimal routing entries in the multicast routing table are added to the multicast forwarding table.

RPF check mechanism

A multicast routing protocol uses reverse path forwarding (RPF) check to ensure the multicast data delivery along the correct paths when the multicast routing protocol creates multicast routing entries based on the existing unicast routes or static multicast routes. RPF check also helps avoid data loops.

A multicast routing protocol uses the following tables to perform an RPF check:

- **Unicast routing table**—Contains unicast routing information.
- **Static multicast routing table**—Contains RPF routes that are manually configured. This table is used for RPF check rather than multicast routing.

RPF check process

When performing an RPF check, the router searches its unicast routing table and static multicast routing table at the same time by using the following process:

1. The router separately chooses each optimal route from the unicast routing table and the static multicast routing table:
   - The router looks up its unicast routing table by using the IP address of the packet source as the destination address, and automatically chooses an optimal unicast route. The outgoing interface of the route is the RPF interface and the next hop is the RPF neighbor. The router considers the path of the packet that the RPF interface receives from the RPF neighbor as the shortest path that leads back to the source.
   - The router looks up its static multicast routing table by using the IP address of the packet source as the source address, and automatically chooses an optimal static multicast route. The route explicitly defines the RPF interface and the RPF neighbor.
2. The router selects one of the two optimal routes as the RPF route according to the following principles:
   - If the router uses the longest prefix match principle, the router selects the matching route as the RPF route. If the routes have the same mask, the router selects the route that has the higher priority as the RPF route. If the routes have the same priority, the static multicast route takes precedence over the unicast route.

    For more information about the route preference, see *Layer 3—IP Routing Configuration Guide*.

    - If the router does not use the longest prefix match principle, the router selects the route that has the higher priority as the RPF route. If the routes have the same priority, the static multicast route takes precedence over the unicast route..

In RPF checks, a "packet source" means different things in different situations:

- For a packet that travels along the SPT from the multicast source to the receivers or to the RP, the packet source is the multicast source.
- For a packet that travels along the RPT from the RP to the receivers, or along the source-side RPT from the multicast source to the RP, the packet source is the RP.
- For a bootstrap message from the BSR, the packet source is the BSR.

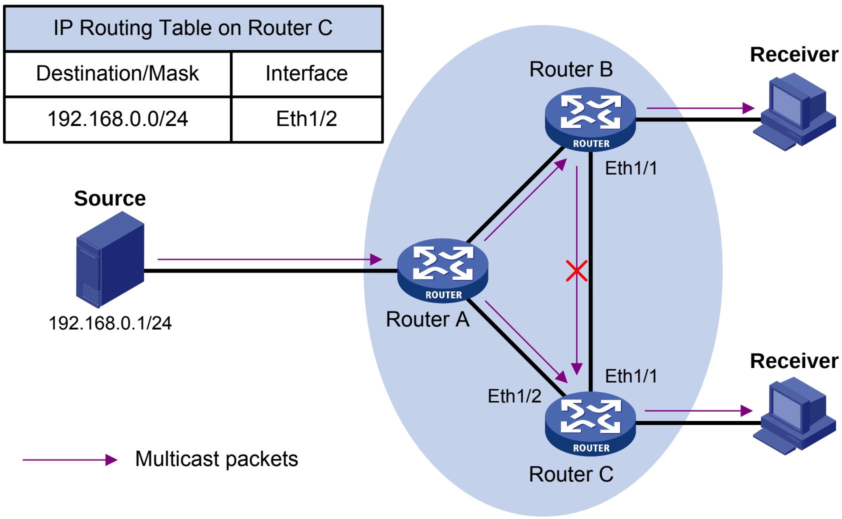
For more information about the concepts of SPT, RPT, source-side RPT, RP, and BSR, see "Configuring PIM."

RPF check implementation in multicast

Implementing an RPF check on each received multicast packet brings a big burden to the router. The use of a multicast forwarding table is the solution to this issue. When the router creates a multicast routing entry and a multicast forwarding entry for a multicast packet, it sets the RPF interface of the packet as the incoming interface of the forwarding entry. After the router receives a multicast packet, it looks up its multicast forwarding table:

- If no forwarding entry matches the packet, the packet undergoes an RPF check. The router creates a multicast routing entry with the RPF interface as the incoming interface and adds the entry into the multicast forwarding table. The process goes as follows:
    - If the interface that received the packet is the RPF interface, the RPF check succeeds and the router forwards the packet out of all the outgoing interfaces.
    - If the interface that received the packet is not the RPF interface, the RPF check fails and the router discards the packet.
- If a forwarding entry matches the packet and the interface that received the packet is the incoming interface of the forwarding entry, the router forwards the packet out of all the outgoing interfaces.
- If a forwarding entry matches the packet but the interface that received the packet is not the incoming interface of the forwarding entry, the multicast packet undergoes an RPF check.
    - If the RPF interface is the incoming interface, it means that the forwarding entry is correct, but the packet traveled along a wrong path. The router discards the packet.
    - If the RPF interface is not the incoming interface, it means that the forwarding entry has expired, and the router replaces the incoming interface with the RPF interface. In this case, if the interface that received the packet is the RPF interface, the router forwards the packet out of all outgoing interfaces. Otherwise, it discards the packet.

Figure 14 RPF check process



IP Routing Table on Router C	
Destination/Mask	Interface
192.168.0.0/24	Eth1/2

As shown in Figure 14, assume that unicast routes are available in the network, and no static multicast routes have been configured on Router C. 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 Ethernet 1/2 as the incoming interface.

- When Ethernet 1/2 of Router C receives a multicast packet, because the interface is the incoming interface of the (S, G) entry, the router forwards the packet out of all outgoing interfaces.
- When Ethernet 1/1 of Router C receives a multicast packet, because the interface is not the incoming interface of the (S, G) entry, the router performs an RPF check on the packet. The router looks up its unicast routing table and finds that the outgoing interface to the source (the RPF interface) is Ethernet 1/2. It means that the (S, G) entry is correct, but the packet traveled along a wrong path. The RPF check fails and the router discards the packet.

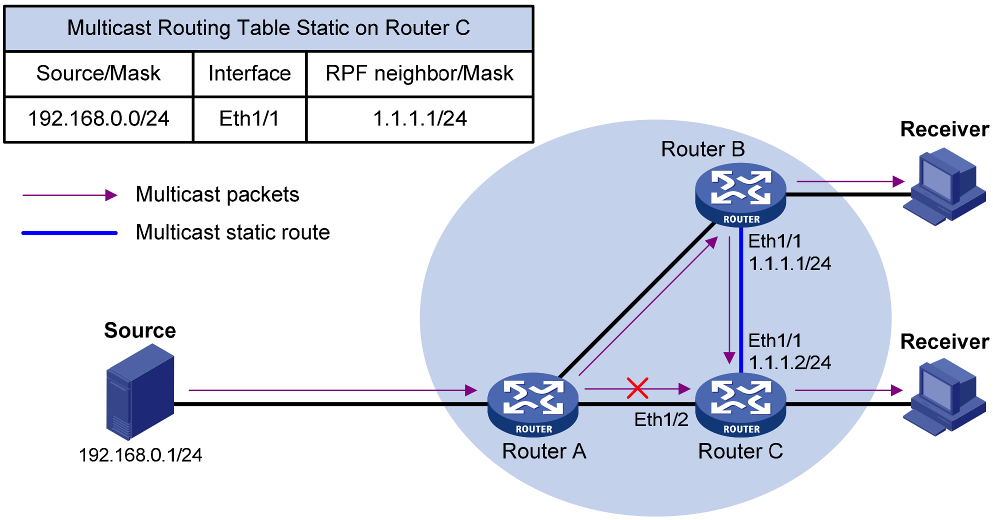
Static multicast routes

Depending on the application environment, a static multicast route can 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 as unicast traffic does. You can configure a static multicast route for a given multicast source to change the RPF route, so that the router creates a transmission path for multicast traffic that is different from the transmission path for unicast traffic.

Figure 15 Changing an RPF route



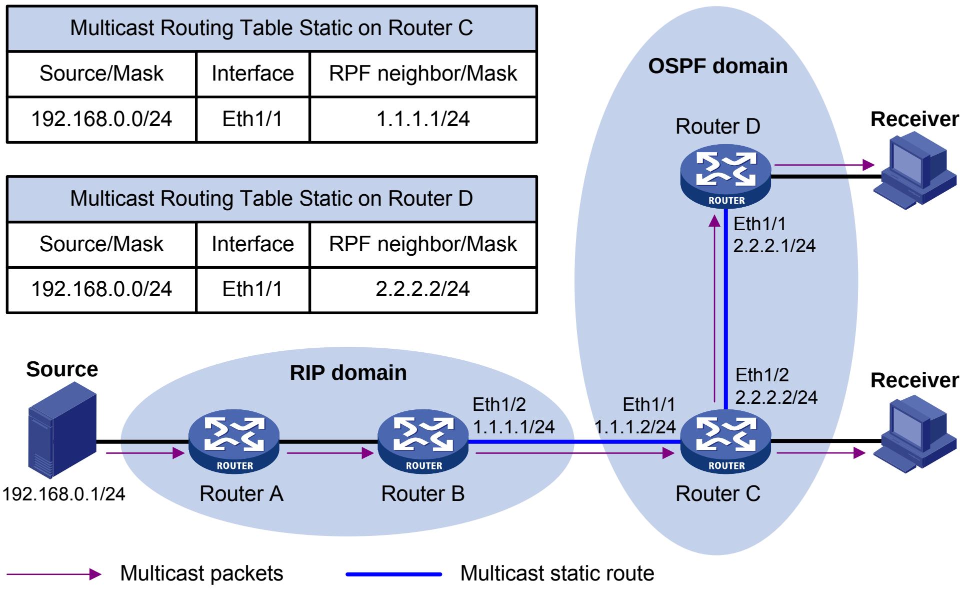
Multicast Routing Table Static on Router C		
Source/Mask	Interface	RPF neighbor/Mask
192.168.0.0/24	Eth1/1	1.1.1.1/24

As shown in Figure 15, when no static multicast route is configured, Router C's RPF neighbor on the path back to the source is Router A, and the multicast data from the source travels through Router A to Router C. When a static multicast route is configured on Router C with Router B as its RPF neighbor on the path back to the source, the multicast data from the source travels along the path: Router A to Router B and then to Router C.

Creating an RPF route

When a unicast route is blocked, multicast forwarding might be stopped due to lack of an RPF route. In this case, you can create an RPF route by configuring a static multicast route for a given multicast source, so that a multicast routing entry is created to guide multicast forwarding.

Figure 16 Creating an RPF route



Multicast Routing Table Static on Router C		
Source/Mask	Interface	RPF neighbor/Mask
192.168.0.0/24	Eth1/1	1.1.1.1/24

Multicast Routing Table Static on Router D		
Source/Mask	Interface	RPF neighbor/Mask
192.168.0.0/24	Eth1/1	2.2.2.2/24

As shown in Figure 16, the RIP domain and the OSPF domain are unicast isolated from each other. When no static multicast route is configured, the receiver hosts in the OSPF domain cannot receive the multicast packets from the multicast source in the RIP domain. If you configure a static multicast 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 receiver hosts can receive the multicast data from the multicast source.

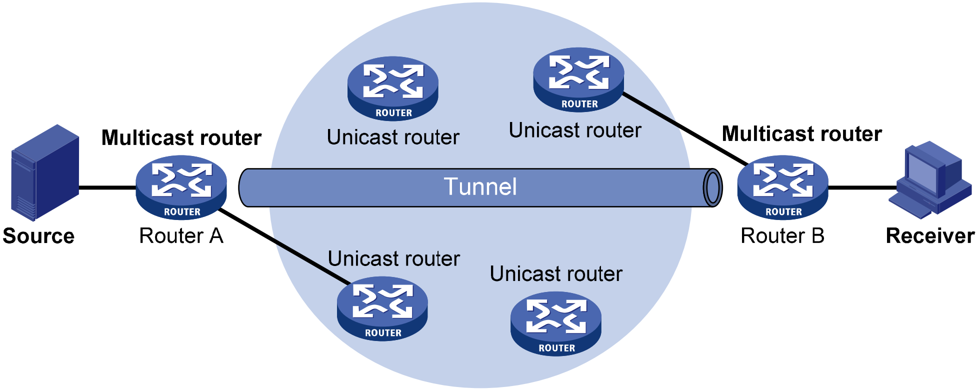
NOTE:

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

Multicast forwarding across unicast subnets

Routers forward the multicast data from a multicast source hop by hop along the forwarding tree, but some routers might not support multicast protocols in a network. When the multicast data is forwarded to a router that does not support IP multicast, the forwarding path is blocked. In this case, you can enable multicast forwarding across two unicast subnets by establishing a tunnel between the routers at the edges of the two unicast subnets.

Figure 17 Multicast data transmission through a tunnel



As shown in Figure 17, with a tunnel established between the multicast routers Router A and Router B, Router A encapsulates the multicast data in unicast IP packets, and forwards them to Router B across the tunnel through unicast routers. Then, Router B strips off the unicast IP header and continues to forward the multicast data to the receiver.

To use this tunnel only for multicast traffic, configure the tunnel as the outgoing interface only for multicast routes.

Configuration task list

Tasks at a glance
(Required.) Enabling IP multicast routing
(Optional.) Configuring multicast routing and forwarding • (Optional.) Configuring static multicast routes • (Optional.) Configuring the RPF route selection rule • (Optional.) Configuring multicast load splitting • (Optional.) Configuring a multicast forwarding boundary • (Optional.) Configuring static multicast MAC address entries

NOTE:

The device can route and forward multicast data only through the primary IP addresses of interfaces, rather than their secondary addresses or unnumbered IP addresses. For more information about primary and secondary IP addresses, and IP unnumbered, see *Layer 3—IP Services Configuration Guide*.

Enabling IP multicast routing

Enable IP multicast routing before you configure any Layer 3 multicast functionality on the public network or VPN instance.

To enable IP multicast routing:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable IP multicast routing and enter MRIB view.	**multicast routing** [**vpn-instance** *vpn-instance-name*]	By default, IP multicast routing is disabled.

Configuring multicast routing and forwarding

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

- Configure a unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Enable PIM-DM or PIM-SM.

Configuring static multicast routes

By configuring a static multicast route for a given multicast source, you can specify an RPF interface or an RPF neighbor for the multicast traffic from that source.

To configure a static multicast route:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure a static multicast route.	**ip rpf-route-static** [**vpn-instance** *vpn-instance-name*] *source-address* { *mask-length* | *mask* } { *rpf-nbr-address* | *interface-type interface-number* } [**preference** *preference*]	By default, no static multicast route exists.
3.	(Optional.) Delete static multicast routes.	• Delete a static multicast route: **undo ip rpf-route-static** [**vpn-instance** *vpn-instance-name*] *source-address* { *mask-length* | *mask* } { *rpf-nbr-address* | *interface-type interface-number* } • Delete all static multicast routes: **delete ip rpf-route-static** [**vpn-instance** *vpn-instance-name*]	N/A

Configuring the RPF route selection rule

You can configure the router to select the RPF route based on the longest prefix match principle. For more information about RPF route selection, see "RPF check process."

To configure a multicast routing policy:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter MRIB view.	**multicast routing** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure the device to select the RPF route based on the longest prefix match.	**longest-match**	By default, the route with the highest priority is selected as the RPF route.

Configuring multicast load splitting

To optimize the traffic delivery for multiple data flows, you can configure load splitting on a per-source basis or on a per-source-and-group basis.

To configure multicast load splitting:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter MRIB view.	**multicast routing** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure multicast load splitting.	**load-splitting** { **source** | **source-group** }	By default, load splitting is disabled.

Configuring a multicast forwarding boundary

A multicast forwarding boundary sets the boundary condition for the multicast groups in the specified range. The multicast data for a multicast group travels within a definite boundary in a network. If the destination address of a multicast packet matches the boundary condition, the packet is not forwarded. If an interface is configured as a multicast boundary, it can no longer forward multicast packets (including packets sent from the local device), nor receive multicast packets.

TIP:

You do not need to enable IP multicast routing before this configuration.

To configure a multicast forwarding boundary:

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

Step	Command	Remarks
3. Configure a multicast forwarding boundary.	**multicast boundary** *group-address* { *mask-length* | *mask* }	By default, no forwarding boundary is configured.

Configuring static multicast MAC address entries

This feature is available only on the MSR series routers with Ethernet Layer 2 switching interface modules. For information about the Ethernet Layer 2 switching interface modules, see *HP MSR Router Series Interface Module Guide*.

In Layer 2 multicast, multicast MAC address entries can be dynamically created or added through Layer 2 multicast protocols (such as IGMP snooping). You can also manually configure static multicast MAC address entries to bind multicast MAC addresses and ports to control the destination ports of the multicast data.

TIP:

- You do not need to enable IP multicast routing before this configuration.
- The multicast MAC address that can be manually configured in the multicast MAC address entry must be unused. (The least significant bit of the most significant octet is 1.)

You can configure static multicast MAC address entries on the specified interface in system view, or on the current interface in interface view.

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

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a static multicast MAC address entry.	**mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	By default, no static multicast MAC address entries exist.

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

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure a static multicast MAC address entry.	**mac-address multicast** *mac-address* **vlan** *vlan-id*	By default, no static multicast MAC address entries exist.

Displaying and maintaining multicast routing and forwarding

CAUTION:

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

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display information about static multicast MAC address table.	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]]
Display information about the interfaces maintained by the MRIB.	**display mrib** [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*]
Display multicast boundary information.	**display multicast** [**vpn-instance** *vpn-instance-name*] **boundary** [*group-address* [*mask-length* | *mask*]] [**interface** *interface-type interface-number*]
Display statistics for multicast forwarding events (MSR2000/MSR3000).	**display multicast** [**vpn-instance** *vpn-instance-name*] **forwarding event**
Display statistics for multicast forwarding events (MSR4000).	**display multicast** [**vpn-instance** *vpn-instance-name*] **forwarding event** [**slot** *slot-number*]
Display multicast forwarding table information (MSR2000/MSR3000).	**display multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number* | **statistics**] *
Display multicast forwarding table information (MSR4000).	**display multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number* | **slot** *slot-number* | **statistics**] *
Display information about the multicast routing table.	**display multicast** [**vpn-instance** *vpn-instance-name*] **routing-table** [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *
Display information about the static multicast routing table.	**display multicast** [**vpn-instance** *vpn-instance-name*] **routing-table static** [*source-address* { *mask-length* | *mask* }]
Display RPF route information about the multicast source.	**display multicast** [**vpn-instance** *vpn-instance-name*] **rpf-info** *source-address* [*group-address*]
Clear statistics for multicast forwarding events.	**reset multicast** [**vpn-instance** *vpn-instance-name*] **forwarding event**

Task	Command
Clear forwarding entries from the multicast forwarding table.	**reset multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table** { { *source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** { *interface-type* *interface-number* } } * | **all** }
Clear routing entries from the multicast routing table.	**reset multicast** [**vpn-instance** *vpn-instance-name*] **routing-table** { { *source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** *interface-type* *interface-number* } * | **all** }

NOTE:

When a routing entry is removed, the associated forwarding entry is also removed. When a forwarding entry is removed, the associated routing entry is also removed.

Configuration examples

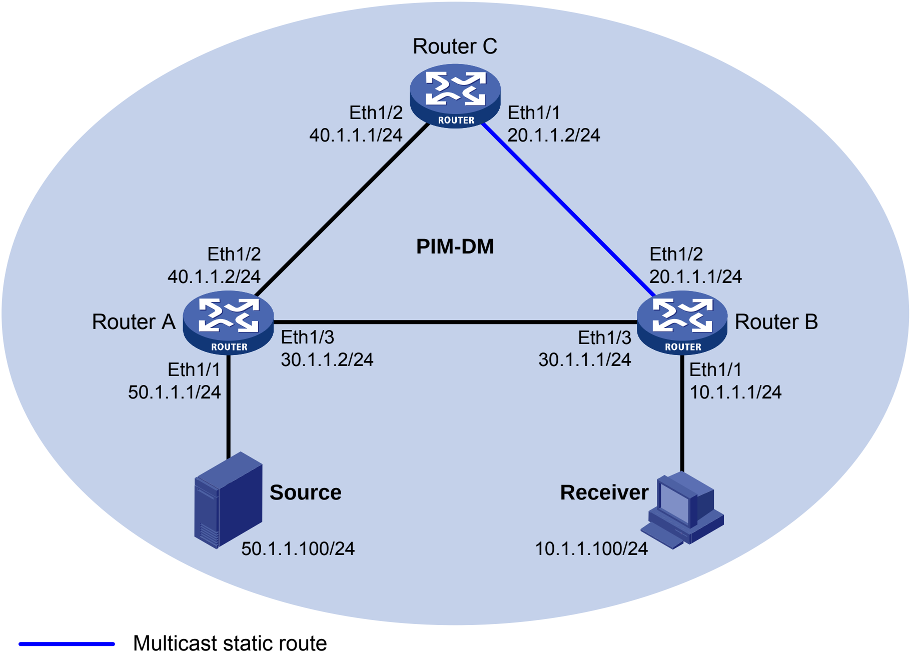
Changing an RPF route

Network requirements

As shown in Figure 18, PIM-DM runs in the network. All routers in the network support multicast. Router A, Router B, and Router C run OSPF. Typically, the receiver host can receive the multicast data from the source through the path: Router A to Router B, which is the same as the unicast route.

Perform the configuration so that the receiver host can receive the multicast data from the source through the path: Router A to Router C to Router B, which is different from the unicast route.

Figure 18 Network diagram



Configuration procedure

1. Configure the IP address and subnet mask for each interface as shown in Figure 18. (Details not shown.)
2. Enable OSPF on the routers in the PIM-DM domain to make sure the network-layer on the PIM-DM network is interoperable and the routing information among the routers can be dynamically updated. (Details not shown.)
3. Enable IP multicast routing, and enable IGMP and PIM-DM:

# On Router B, enable IP multicast routing globally, enable IGMP on Ethernet 1/1, and enable PIM-DM on each interface.

```
<RouterB> system-view
[RouterB] multicast routing
[RouterB-mrib] quit
[RouterB] interface ethernet 1/1
[RouterB-Ethernet1/1] igmp enable
[RouterB-Ethernet1/1] pim dm
[RouterB-Ethernet1/1] quit
[RouterB] interface ethernet 1/2
[RouterB-Ethernet1/2] pim dm
[RouterB-Ethernet1/2] quit
[RouterB] interface ethernet 1/3
[RouterB-Ethernet1/3] pim dm
[RouterB-Ethernet1/3] quit
```

# On Router A, enable IP multicast routing globally and enable PIM-DM on each interface.

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] pim dm
[RouterA-Ethernet1/1] quit
[RouterA] interface ethernet 1/2
[RouterA-Ethernet1/2] pim dm
[RouterA-Ethernet1/2] quit
[RouterA] interface ethernet 1/3
[RouterA-Ethernet1/3] pim dm
[RouterA-Ethernet1/3] quit
```

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

# Use the **display multicast rpf-info** command to display the RPF route to the source on Router B.

```
[RouterB] display multicast rpf-info 50.1.1.100
 RPF information about source 50.1.1.100:
     RPF interface: Ethernet1/3, 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 Router B is contributed by a unicast routing protocol and the RPF neighbor is Router A.

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

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

Verifying the configuration

# Use the **display multicast rpf-info** command on Router B to display information about the RPF route to the source.

```
[RouterB] display multicast rpf-info 50.1.1.100
 RPF information about source 50.1.1.100:
     RPF interface: Ethernet1/2, 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 the following:

- The RPF route on Router B is the configured static multicast route.
- The RPF neighbor of Router B is Router C.

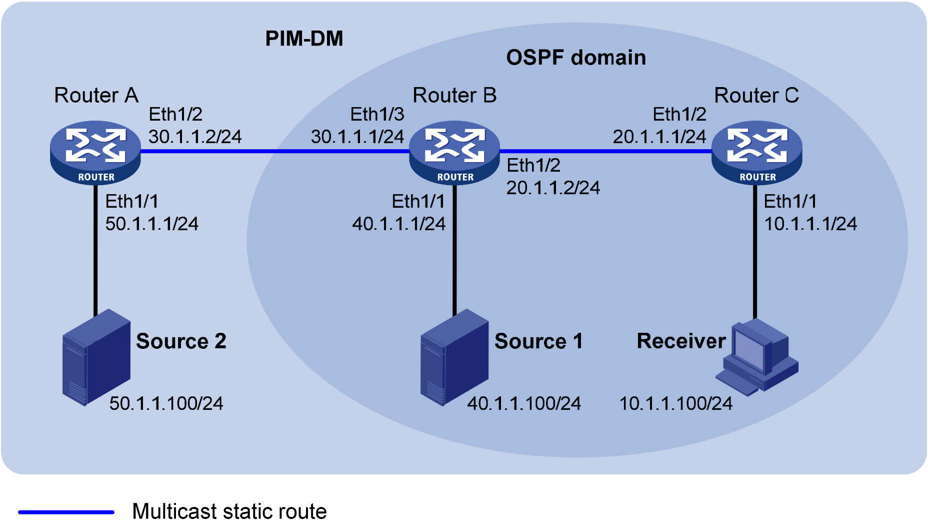
Creating an RPF route

Network requirements

As shown in Figure 19, PIM-DM runs in the network and all routers in the network support IP multicast. Router B and Router C run OSPF, and have no unicast routes to Router A. Typically, the receiver host receives the multicast data from the source 1 in the OSPF domain.

Perform the configuration so that the receiver host can receive multicast data from the source 2, which is outside the OSPF domain.

Figure 19 Network diagram



Configuration procedure

1. Configure the IP address and subnet mask for each interface as shown in Figure 19. (Details not shown.)

2. Enable OSPF on Router B and Router C to make sure the network-layer on the PIM-DM network is interoperable and the routing information among the routers can be dynamically updated. (Details not shown.)
3. Enable IP multicast routing, and enable IGMP and PIM-DM:

   # On Router C, enable IP multicast routing globally, enable IGMP on Ethernet 1/1, and enable PIM-DM on each interface.

   ```
   <RouterC> system-view
   [RouterC] multicast routing
   [RouterC-mrib] quit
   [RouterC] interface ethernet 1/1
   [RouterC-Ethernet1/1] igmp enable
   [RouterC-Ethernet1/1] pim dm
   [RouterC-Ethernet1/1] quit
   [RouterC] interface ethernet 1/2
   [RouterC-Ethernet1/2] pim dm
   [RouterC-Ethernet1/2] quit
   ```

   # On Router A, enable IP multicast routing globally and enable PIM-DM on each interface.

   ```
   <RouterA> system-view
   [RouterA] multicast routing
   [RouterA-mrib] quit
   [RouterA] interface ethernet 1/1
   [RouterA-Ethernet1/1] pim dm
   [RouterA-Ethernet1/1] quit
   [RouterA] interface ethernet 1/2
   [RouterA-Ethernet1/2] pim dm
   [RouterA-Ethernet1/2] quit
   ```

   # Enable IP multicast routing and PIM-DM on Router B in the same way Router A is configured. (Details not shown.)

   # Use the **display multicast rpf-info** command on Router B and Router C to display information about their RPF routes to the source 2.

   ```
   [RouterB] display multicast rpf-info 50.1.1.100
   [RouterC] display multicast rpf-info 50.1.1.100
   ```

   No output is displayed, so no RPF routes to the source 2 exist on Router B and Router C.
4. Configure a static multicast route:

   # Configure a static multicast route on Router B, specifying Router A as its RPF neighbor on the route to the source 2.

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

   # Configure a static multicast route on Router C, specifying Router B as its RPF neighbor on the route to the source 2.

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

Verifying the configuration

Use the **display multicast rpf-info** command on Router B and Router C to display information about their RPF routes to the source 2.

```
[RouterB] display multicast rpf-info 50.1.1.100
 RPF information about source 50.1.1.100:
     RPF interface: Ethernet1/3, 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
[RouterC] display multicast rpf-info 50.1.1.100
 RPF information about source 50.1.1.100:
     RPF interface: Ethernet1/2, 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
```

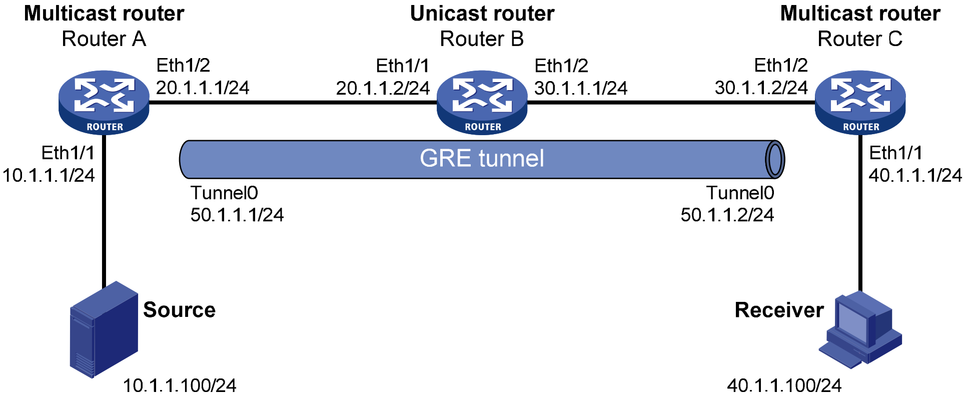
The output shows that the RPF routes to the source 2 exist on Router B and Router C. These RPF routes are the configured static multicast routes.

Multicast forwarding over GRE tunnels

Network requirements

As shown in Figure 20, multicast routing and PIM-DM are enabled on Router A and Router C. Router B does not support multicast. OSPF is running on Router A, Router B, and Router C. Configure a GRE tunnel so that the receiver host can receive the multicast data from the source.

Figure 20 Network diagram



Configuration procedure

1. Configure the IP address and mask for each interface as shown in Figure 20. (Details not shown.)
2. Enable OSPF on routers to make sure the network-layer among the routers is interoperable and the routing information among the routers can be dynamically updated. (Details not shown.)
3. Configure a GRE tunnel:

   # Create interface Tunnel 0 on Router A and specify the tunnel encapsulation mode as GRE over IPv4.

   ```
   <RouterA> system-view
   [RouterA] interface tunnel 0 mode gre
   ```

   # Configure the IP address for interface Tunnel 0 on Router A and specify its source and destination addresses.

   ```
   [RouterA-Tunnel0] ip address 50.1.1.1 24
   ```

```
[RouterA-Tunnel0] source 20.1.1.1
[RouterA-Tunnel0] destination 30.1.1.2
[RouterA-Tunnel0] quit
```

# Create interface Tunnel 0 on Router C and specify the tunnel encapsulation mode as GRE over IPv4.

```
<RouterC> system-view
[RouterC] interface tunnel 0 mode gre
```

# Configure the IP address for interface Tunnel 0 and specify its source and destination addresses.

```
[RouterC-Tunnel0] ip address 50.1.1.2 24
[RouterC-Tunnel0] source 30.1.1.2
[RouterC-Tunnel0] destination 20.1.1.1
[RouterC-Tunnel0] quit
```

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

# On Router A, enable multicast routing globally and enable PIM-DM on each interface.

```
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] pim dm
[RouterA-Ethernet1/1] quit
[RouterA] interface ethernet 1/2
[RouterA-Ethernet1/2] pim dm
[RouterA-Ethernet1/2] quit
[RouterA] interface tunnel 0
[RouterA-Tunnel0] pim dm
[RouterA-Tunnel0] quit
```

# On Router C, enable multicast routing globally, enable IGMP on Ethernet 1/1, and enable PIM-DM on each interface.

```
[RouterC] multicast routing
[RouterC-mrib] quit
[RouterC] interface ethernet 1/1
[RouterC-Ethernet1/1] igmp enable
[RouterC-Ethernet1/1] pim dm
[RouterC-Ethernet1/1] quit
[RouterC] interface ethernet 1/2
[RouterC-Ethernet1/2] pim dm
[RouterC-Ethernet1/2] quit
[RouterC] interface tunnel 0
[RouterC-Tunnel0] pim dm
[RouterC-Tunnel0] quit
```

5. On Router C, configure a static multicast route to specify its RPF neighbor toward the source is interface Tunnel 0 on Router A.

```
[RouterC] ip rpf-route-static 10.1.1.0 24 50.1.1.1
```

Verifying the configuration

The source sends the multicast data to the multicast group 225.1.1.1 and the receiver host can receive the multicast data after joining the multicast group. You can use the **display pim routing-table** command to display PIM routing table information on routers. For example:

# Display PIM routing table information on Router C.

```
[RouterC] display pim routing-table
 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: Ethernet1/1
             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: Ethernet1/1
             Protocol: pim-dm, UpTime: 00:04:25, Expires: never
```

The output shows that Router A is the RPF neighbor of Router C and the multicast data from Router A is delivered over a GRE tunnel to Router C.

Troubleshooting multicast routing and forwarding

Static multicast route failure

Symptom

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

Analysis

- If a static multicast route is not correctly configured or updated to match the current network conditions, it does not exist in the static multicast routing table.
- If a better route is found, the static multicast route might also fail.

Solution

1. Use the **display multicast routing-table static** command to display information about static multicast routes to verify that the static multicast route has been correctly configured and the route entry exists in the static multicast routing table.
2. Check the type of the interface that connects the static multicast route to the RPF neighbor. If the interface is not a point-to-point interface, be sure to specify the address for the RPF neighbor.

Configuring IGMP

Overview

Internet Group Management Protocol (IGMP) establishes and maintains the multicast group memberships between a Layer 3 multicast device and its directly connected hosts.

IGMP has three versions:

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

All IGMP versions support the ASM model. In addition to the ASM model, IGMPv3 can directly implement the SSM model. IGMPv1 and IGMPv2 must work with the IGMP SSM mapping function to implement the SSM model. For more information about the ASM and SSM models, see "Multicast overview."

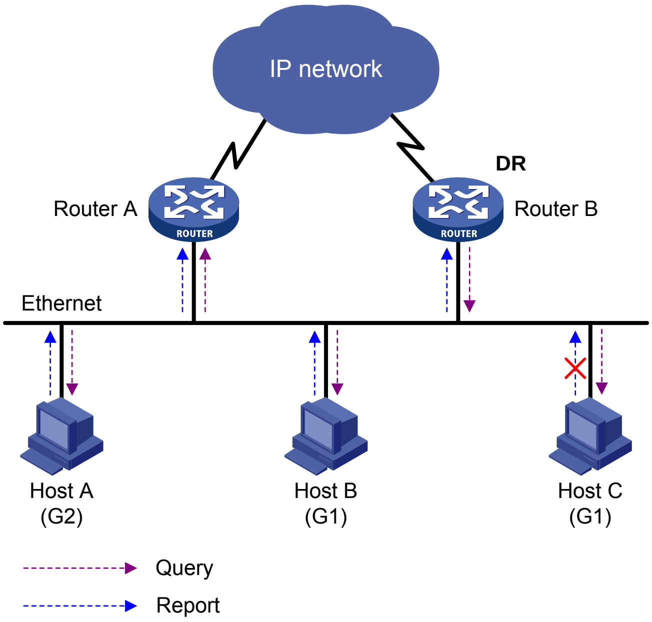
IGMPv1 overview

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

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

In IGMPv1, the designated router (DR) elected by the multicast routing protocol (such as PIM) serves as the IGMP querier. For more information about DR, see "Configuring PIM."

Figure 21 IGMP queries and reports



As shown in Figure 21, Host B and Host C are interested in the multicast data addressed to the multicast group G1, and Host A is interested in the multicast data addressed to G2. The following process describes how the hosts join the multicast groups and how the IGMP querier (Router B in Figure 21) maintains the multicast group memberships:

1. The hosts send unsolicited IGMP reports to the multicast groups they want to join without having to wait for the IGMP queries from the IGMP querier.
2. The IGMP querier periodically multicasts IGMP queries (with the destination address of 224.0.0.1) to all hosts and routers on the local subnet.
3. After receiving a query message, Host B or Host C (the host whose delay timer expires first) sends an IGMP report to the multicast group G1 to announce its membership for G1. This example assumes that Host B sends the report message. After receiving the report from Host B, Host C suppresses its own report for G1 because the IGMP routers (Router A and Router B) already know that G1 has at least one member host on the local subnet. This IGMP report suppression mechanism helps reduce traffic on the local subnet.
4. At the same time, Host A sends a report to the multicast group G2 after receiving a query message.
5. Through the query and response process, the IGMP routers (Router A and Router B) determine that the local subnet has members of G1 and G2, and the multicast routing protocol (PIM, for example) on the routers generates (*, G1) and (*, G2) multicast forwarding entries, where asterisk (*) represents any multicast source. These entries are the basis for subsequent multicast forwarding.
6. When the multicast data addressed to G1 or G2 reaches an IGMP router, the router looks up the multicast forwarding table and forwards the multicast data to the local subnet based on the (*, G1) or (*, G2) entry. Then, the receivers on the subnet can receive the data.

IGMPv1 does not define a leave group message (often called a "leave message"). When an IGMPv1 host is leaving a multicast group, it stops sending reports to that multicast group. If the subnet has no members for a multicast group, the IGMP routers will not receive any report addressed to that multicast group. In this case, the routers clear the information for that multicast group after a period of time.

IGMPv2 enhancements

Backwards-compatible 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 that run IGMP 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 to be 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 the other IGMPv2 routers become non-queriers.
3. All the non-queriers start a timer, known as an "other querier present timer." If a router receives an IGMP query from the querier before the timer expires, it resets this timer. Otherwise, it considers 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 routers. The multicast routers determine whether a group has members by using the maximum response delay. 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. After receiving the leave message, the querier sends a configurable number of group-specific queries to the group that the host is leaving. Both the destination address field and the group address field of the message are the address of the multicast group that is being queried.
3. One of the remaining members (if any on the subnet) of the group should send a membership report within the maximum response delay advertised in the query messages.
4. If the querier receives a membership report for the group before the maximum response delay timer expires, it maintains the memberships for the group. Otherwise, the querier assumes that the local subnet has no member hosts for the group and stops maintaining the memberships for the group.

IGMPv3 enhancements

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

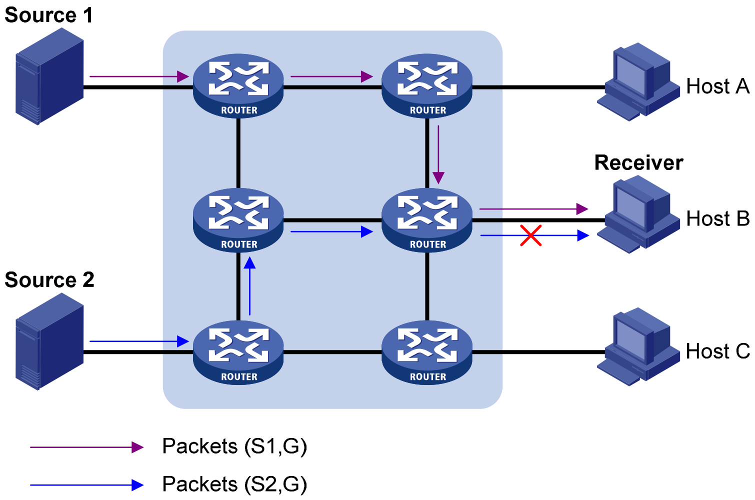
Enhancements in control capability of hosts

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

- If the host expects 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 the host expects 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 22, the network comprises two multicast sources, Source 1 (S1) and Source 2 (S2), both of which can send multicast data to the multicast group G. Host B is interested in the multicast data that Source 1 sends to G but not in the data from Source 2.

Figure 22 Flow paths of source-and-group-specific multicast traffic



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

When IGMPv3 runs between the hosts and routers, Host B can explicitly express that it needs to receive the multicast data that Source 1 sends to the 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

- Query message carrying the source addresses

  Compatible with IGMPv1 and IGMPv2, IGMPv3 supports general queries and group-specific queries. It also introduces 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.
- Reports containing multiple group records

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

  Group records include the following categories:

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

IGMP support for VPNs

IGMP maintains group memberships on a per-interface base. After receiving an IGMP message on an interface, IGMP processes the packet within the VPN to which the interface belongs. IGMP only communicates with other multicast protocols within the same VPN instance.

Protocols and standards

- RFC 1112, *Host Extensions for IP Multicasting*
- RFC 2236, *Internet Group Management Protocol, Version 2*
- RFC 3376, *Internet Group Management Protocol, Version 3*

IGMP configuration task list

Task at a glance
Configuring basic IGMP functions • (Required.) Enabling IGMP • (Optional.) Specifying the IGMP version • (Optional.) Configuring an interface as a static member interface • (Optional.) Configuring a multicast group filter
Adjusting IGMP performance (Optional.) Enabling IGMP fast-leave processing

Configuring basic IGMP functions

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

- Configure any unicast routing protocol so that all devices are interoperable at the network layer.
- Configure PIM.
- Determine the IGMP version.

- Determine the multicast group and multicast source addresses for static group member configuration.
- Determine the ACL for multicast group filtering.

Enabling IGMP

To configure IGMP, enable IGMP on the interface where the multicast group memberships are established and maintained.

To enable IGMP:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable IP multicast routing and enter MRIB view.	**multicast routing** [**vpn-instance** *vpn-instance-name*]	Disabled by default.
3.	Return to system view.	**quit**	N/A
4.	Enter interface view.	**interface** *interface-type interface-number*	N/A
5.	Enable IGMP.	**igmp enable**	Disabled by default.

Specifying the IGMP version

Because the protocol packets of different IGMP versions vary in structure and type, specify the same IGMP version for all routers on the same subnet. Otherwise, IGMP cannot operate correctly.

To specify an IGMP version:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter interface view.	**interface** *interface-type interface-number*	N/A
3.	Specify an IGMP version.	**igmp version** *version-number*	IGMPv2 by default.

Configuring an interface as a static member interface

You can configure an interface as a static member of a multicast group or a multicast source and group, so that the interface can receive multicast data addressed to that multicast group for the purpose of testing multicast data forwarding.

Configuration guidelines

- A static member interface has the following restrictions:
  - If the interface is IGMP and PIM-SM enabled, it must be a PIM-SM DR.
  - If the interface is IGMP enabled but not PIM-SM enabled, it must be an IGMP querier.

  For more information about PIM-SM and DR, see "Configuring PIM."

- A static member interface does not respond to queries that the IGMP querier sends. When you configure an interface as a static member or cancel this configuration on the interface, the interface does not send any IGMP report or IGMP leave message without a request. This is because the interface is not a real member of the multicast group or the multicast source and group.

Configuration procedure

To configure an interface as a static member interface:

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

Configuring a multicast group filter

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

To configure a multicast group filter:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Configure a multicast group filter.	**igmp group-policy** *acl-number* [*version-number*]	By default, no multicast group filter is configured on any interface. Hosts attached to an interface can join any multicast group.

NOTE:

If you configure the interface as a static member interface for a multicast group or a multicast source and group, this configuration does not take effect on the multicast group or the multicast source and group.

Adjusting IGMP performance

Before adjusting IGMP performance, complete the following tasks:

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

Enabling IGMP fast-leave processing

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

With IGMP fast-leave processing enabled, after receiving an IGMP leave message from a host, the IGMP querier directly sends a leave notification to the upstream without sending IGMP group-specific queries or IGMP group-and-source-specific queries. This reduces leave latency and preserves the network bandwidth.

The IGMP fast-leave processing configuration takes effect only if the device is running IGMPv2 or IGMPv3.

To enable IGMP fast-leave processing:

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

Displaying and maintaining IGMP

△ CAUTION:

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

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display IGMP group information.	**display igmp** [**vpn-instance** *vpn-instance-name*] **group** [*group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]
Display IGMP information.	**display igmp**[**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**]
Remove all the dynamic IGMP group entries of an IGMP group or all IGMP groups.	**reset igmp** [**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* }]] } }

NOTE:

The **reset igmp group** command cannot remove static IGMP group entries.

IGMP configuration example

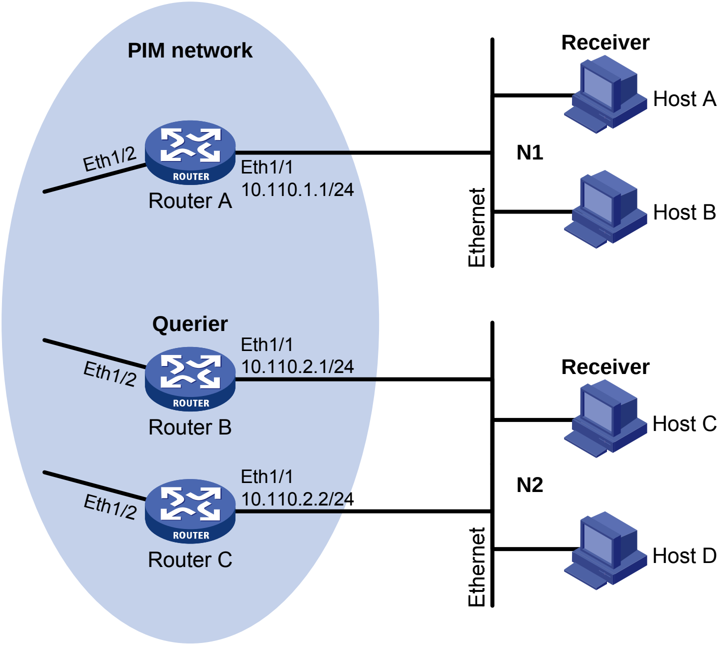
Network requirements

AS shown in Figure 23, VOD streams are sent to receiver hosts in multicast. Receiver hosts of different organizations form stub networks N1 and N2. Host A and Host C are receiver hosts in N1 and N2, respectively.

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

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

Figure 23 Network diagram



Configuration procedure

1. Assign the IP address and subnet mask of each interface as shown in Figure 23. (Details not shown.)
2. Configure OSPF on the PIM network to make sure the network-layer is interoperable on the PIM network and the routing information among the routers can be dynamically updated. (Details not shown.)
3. Enable IP multicast routing, and enable IGMP and PIM-DM:

   # On Router A, enable IP multicast routing globally, enable IGMP on Ethernet 1/1, and enable PIM-DM on each interface.

   ```
   <RouterA> system-view
   [RouterA] multicast routing
   [RouterA-mrib] quit
   [RouterA] interface ethernet 1/1
   [RouterA-Ethernet1/1] igmp enable
   ```

```
[RouterA-Ethernet1/1] pim dm
[RouterA-Ethernet1/1] quit
[RouterA] interface ethernet 1/2
[RouterA-Ethernet1/2] pim dm
[RouterA-Ethernet1/2] quit
```

# On Router B, enable IP multicast routing globally, enable IGMP on Ethernet 1/1, and enable PIM-DM on each interface.

```
<RouterB> system-view
[RouterB] multicast routing
[RouterB-mrib] quit
[RouterB] interface ethernet 1/1
[RouterB-Ethernet1/1] igmp enable
[RouterB-Ethernet1/1] pim dm
[RouterB-Ethernet1/1] quit
[RouterB] interface ethernet 1/2
[RouterB-Ethernet1/2] pim dm
[RouterB-Ethernet1/2] quit
```

# On Router C, enable IP multicast routing globally, enable IGMP on Ethernet 1/1, and enable PIM-DM on each interface.

```
<RouterC> system-view
[RouterC] multicast routing
[RouterC-mrib] quit
[RouterC] interface ethernet 1/1
[RouterC-Ethernet1/1] igmp enable
[RouterC-Ethernet1/1] pim dm
[RouterC-Ethernet1/1] quit
[RouterC] interface ethernet 1/2
[RouterC-Ethernet1/2] pim dm
[RouterC-Ethernet1/2] quit
```

4. Configure a multicast group filter on Router A, so that the hosts connected to Ethernet 1/1 can join the multicast group 224.1.1.1 only.

```
[RouterA] acl number 2001
[RouterA-acl-basic-2001] rule permit source 224.1.1.1 0
[RouterA-acl-basic-2001] quit
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] igmp group-policy 2001
[RouterA-Ethernet1/1] quit
```

Verifying the configuration

Display IGMP information on Ethernet 1/1 of Router B.

```
[RouterB] display igmp interface ethernet 1/1
 Ethernet1/1(10.110.2.1):
   IGMP is enabled.
   IGMP version: 2
   Query interval for IGMP: 125s
   Other querier present time for IGMP: 255s
   Maximum query response time for IGMP: 10s
   Querier for IGMP: 10.110.2.1 (This router)
  IGMP groups reported in total: 1
```

Troubleshooting IGMP

No membership information on the receiver-side router

Symptom

When a host sends a report for joining the 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. IGMP must be enabled on the interface that connects to the host.
- If the IGMP version on the router interface is lower than that on the host, the router cannot recognize the IGMP report from the host.
- If you have configured the **igmp group-policy** command on the interface, the interface cannot receive report messages that failed to pass filtering.

Solution

1. Use the **display igmp interface** command to verify that the networking, interface connection, and IP address configuration are correct. If the command does not produce output, the interface is in an abnormal state. The reason might be that you have configured the **shutdown** command on the interface, the interface is not correctly connected, or the IP address configuration is not correctly completed.
2. Use the **display current-configuration** command to verify that multicast routing is enabled. If it is not enabled, use the **multicast routing** command in system view to enable IP multicast routing. In addition, verify that IGMP is enabled on the associated interfaces.
3. Use the **display igmp interface** command to verify that the IGMP version on the interface is lower than that on the host.
4. Use the **display current-configuration interface** command to verify that no ACL rule has been configured to filter out the reports sent by the host to the multicast group G.

Inconsistent membership information on the 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. Inconsistent IGMP interface parameter configurations for routers on the same subnet will result in inconsistency of memberships.

- In addition, although IGMP routers are partially compatible with hosts that separately run different versions of IGMP, all routers on the same subnet must run the same version of IGMP. Inconsistent IGMP versions running on routers on the same subnet leads to inconsistency of IGMP memberships.

Solution

1. Use the **display current-configuration** command to verify the IGMP information on the interfaces.
2. Use the **display igmp interface** command on all routers on the same subnet to verify the IGMP-related timer settings. Make sure the settings are consistent on all the routers.
3. Use the **display igmp interface** command to verify that all the routers on the same subnet are running the same IGMP version.

Configuring PIM

Overview

Protocol Independent Multicast (PIM) provides IP multicast forwarding by leveraging unicast static routes or unicast routing tables generated by any unicast routing protocol, such as RIP, OSPF, IS-IS, or BGP. PIM is not dependent on any particular unicast routing protocol, and it uses the underlying unicast routing to generate a routing table with routes.

PIM uses the RPF mechanism to implement multicast forwarding. When a multicast packet arrives on an interface of the device, it undergoes an RPF check. If the RPF check succeeds, the device creates a multicast routing entry and forwards the packet. If the RPF check fails, the device discards the packet. For more information about RPF, see "Configuring multicast routing and forwarding."

Based on the implementation mechanism, PIM includes the following categories:

- Protocol Independent Multicast–Dense Mode (PIM-DM)
- Protocol Independent Multicast–Sparse Mode (PIM-SM)
- Protocol Independent Multicast Source-Specific Multicast (PIM-SSM)

In this document, a PIM domain refers to a network composed of PIM routers.

PIM-DM overview

PIM-DM 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 all downstream nodes want to receive multicast data when a source starts sending, so multicast data is flooded to all downstream nodes on the network.
- Branches without downstream receivers are pruned from the forwarding trees, leaving only those branches that contain receivers.
- The pruned state of a branch has a finite holdtime timer. When the timer expires, multicast data is again forwarded to the pruned branch. This flood-and-prune cycle takes place periodically to maintain the forwarding branches.
- To reduce join latency when a new receiver on a previously pruned branch joins a multicast group, PIM-DM uses a graft mechanism to turn the pruned branch into a forwarding branch.

In PIM-DM, the multicast forwarding paths for a multicast group constitutes a source tree, which is rooted at the multicast source and has multicast group members as its "leaves." Because the source tree consists of the shortest paths from the multicast source to the receivers, it is also called a "shortest path tree (SPT)."

The operating mechanism of PIM-DM is summarized as follows:

- Neighbor discovery
- SPT building
- Graft
- Assert

Neighbor discovery

In a PIM domain, each interface that runs PIM on a router periodically multicasts PIM hello messages to all other PIM routers (identified by the address 224.0.0.13) on the local subnet to discover PIM neighbors, maintain PIM neighboring relationship with other routers, and build and maintain SPTs.

SPT building

The process of building an SPT is the flood-and-prune process:

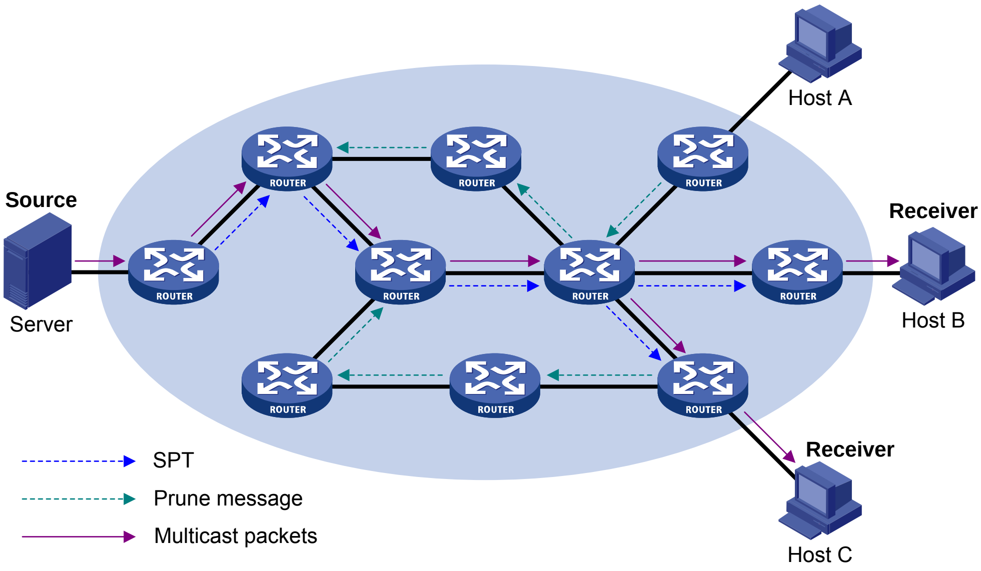
1. In a PIM-DM domain, when the multicast source S sends multicast data to the multicast group G, the multicast data is flooded throughout the domain. A router performs an RPF check for the multicast data. If the RPF check succeeds, the router creates an (S, G) entry and forwards the data to all downstream nodes in the network. In the flooding process, all the routers in the PIM-DM domain create the (S, G) entry.
2. The nodes without downstream receivers are pruned. A router that has no downstream receivers sends a prune message to the upstream node to remove the interface that receives the prune message from the (S, G) entry. In this way, the upstream stream node stops forwarding subsequent packets addressed to that multicast group down to this node.

NOTE:

An (S, G) entry contains a multicast source address S, a multicast group address G, an outgoing interface list, and an incoming interface.

A prune process is initiated by a leaf router. As shown in Figure 24, the router interface that does not have any downstream receivers initiates a prune process by sending a prune message toward the multicast source. This prune process goes on until only necessary branches are left in the PIM-DM domain, and these necessary branches constitute an SPT.

Figure 24 SPT building



The pruned state of a branch has a finite holdtime timer. When the timer expires, multicast data is again forwarded to the pruned branch. The flood-and-prune cycle takes place periodically to maintain the forwarding branches.

Graft

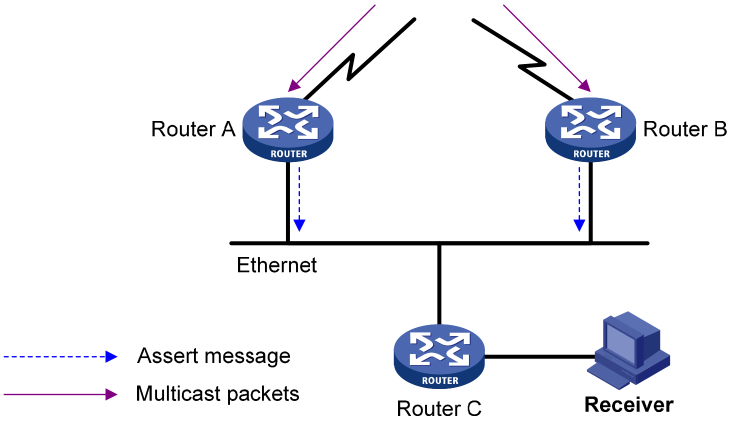
To reduce the join latency when a new receiver on a previously pruned branch joins a multicast group, PIM-DM uses a graft mechanism to turn the pruned branch into a forwarding branch, as follows:

1. The node that needs to receive the multicast data sends a graft message to its upstream node, telling it to rejoin the SPT.
2. After receiving this graft message, the upstream node adds the interface that received the graft message into the outgoing interface list of the (S, G) entry for the multicast group, and then sends 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 continues to send graft messages at a configurable interval until it receives an acknowledgment from its upstream node.

Assert

On a subnet with more than one multicast router, the assert mechanism shuts off duplicate multicast flows to the network. It does this by electing a unique multicast forwarder for the subnet.

Figure 25 Assert mechanism



As shown in Figure 25, after Router A and Router B receive an (S, G) packet from the upstream node, they both forward the packet to the local subnet. As a result, the downstream node Router C receives two identical multicast packets, and both Router A and Router B, on their own downstream interfaces, receive a duplicate packet forwarded by the other. After detecting this condition, both routers send an assert message to all PIM routers (224.0.0.13) on the local subnet through the 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 unicast route/MBGP route/static multicast route to the multicast source. By comparing these parameters, either Router A or Router B becomes the unique forwarder of the subsequent (S, G) packets on the shared-media LAN. The comparison process is as follows:

1. The router with a higher preference to the multicast source wins.
2. If both routers have the same preference to the source, the router with a smaller metric to the multicast source wins.
3. If a tie exists in route metric to the multicast source, the router with a higher IP address on the downstream interface wins.

PIM-SM overview

PIM-DM uses the flood-and-prune cycles to build SPTs for multicast data forwarding. Although an SPT has the shortest paths from the multicast source to the receivers, it is built with a low efficiency and is not suitable for large- and medium-sized networks.

PIM-SM uses the pull mode for multicast forwarding, and it is suitable for large- 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 multicast data. In the PIM-SM mode, a host must express its interest in the multicast data for a multicast group before the data is forwarded to it. PIM-SM implements multicast forwarding by building and maintaining rendezvous point trees (RPTs). An RPT is rooted at a router that has been configured as the rendezvous point (RP) for a multicast group, and the multicast data to the group is forwarded by the RP to the receivers along the RPT.
- When a receiver expresses it interest in the multicast data addressed to a specific multicast group, the receiver-side designated router (DR) sends a join message to the RP for the 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 data to a multicast group, the source-side DR must register the multicast source with the RP by unicasting register messages to the RP. The multicast source stops sending until it receives a register-stop message from the RP. When the RP receives the register message, it triggers the establishment of an SPT. Then, the multicast source sends subsequent multicast packets along the SPT to the RP. After reaching the RP, the multicast packet is duplicated and delivered to the receivers along the RPT.

Multicast data is replicated wherever the RPT branches, and this process automatically repeats until the multicast data reaches the receivers.

The operating mechanism of PIM-SM is summarized as follows:

- Neighbor discovery
- DR election
- RP discovery
- RPT building
- Multicast source registration
- Switchover to SPT
- Assert

Neighbor discovery

PIM-SM uses a similar neighbor discovery mechanism as PIM-DM does. For more information, see "Neighbor discovery."

DR election

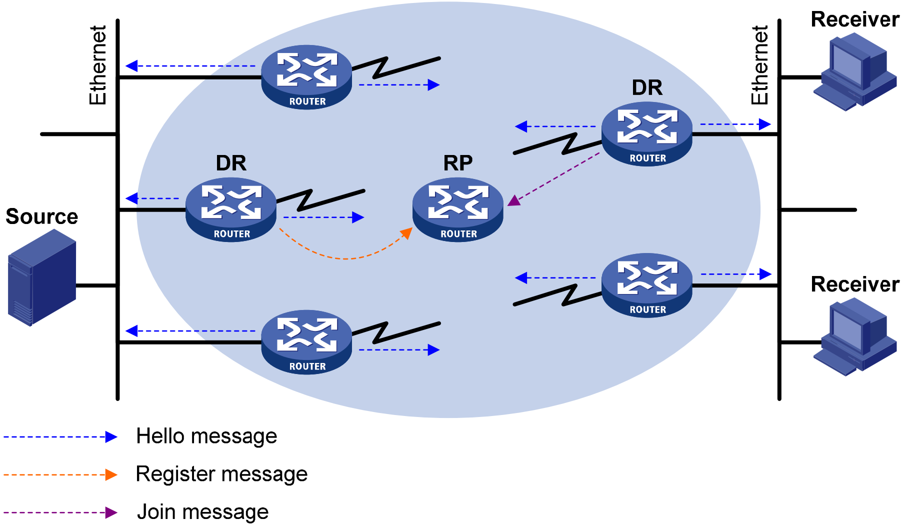
On a shared-media LAN like Ethernet, only a DR forwards the multicast data. A DR is required in both the source-side network and receiver-side network. A source-side DR acts on behalf of the multicast source to send register messages to the RP, and the receiver-side DR acts on behalf of the receiver hosts to send join messages to the RP.

PIM-DM does not require a DR. However, if IGMPv1 runs on any shared-media LAN in a PIM-DM domain, a DR must be elected to act as the IGMPv1 querier for the LAN. For more information about IGMP, see "Configuring IGMP."

IMPORTANT:

IGMP must be enabled on the device that acts as the receiver-side DR. Otherwise, the receiver hosts attached to the DR cannot join any multicast groups.

Figure 26 DR election



As shown in Figure 26, the DR election process is as follows:

1. The routers on the shared-media LAN send hello messages to one another. The hello messages contain the priority for DR election. The router with the highest DR priority is elected as the DR.
2. In the case of a tie in the 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 wins the DR election.

If the DR fails, its PIM neighbor lifetime expires and the other routers will initiate to elect a new DR.

RP discovery

An RP is the core of a PIM-SM domain. For a small-sized, simple network, one RP is enough for multicast forwarding throughout the network. In this case, you can specify a static RP on each router in the PIM-SM domain. However, in a PIM-SM network that covers a wide area, a huge amount of multicast data is forwarded by the RP. To lessen the RP burden and optimize the topological structure of the RPT, you can configure multiple candidate-RPs (C-RPs) in a PIM-SM domain, and use the bootstrap mechanism to dynamically elect RPs. An elected RP provides services for a different multicast group. For this purpose, you must configure a bootstrap router (BSR). A BSR serves as the administrative core of a PIM-SM domain. A PIM-SM domain has only one BSR, but can have multiple candidate-BSRs (C-BSRs) so that, if the BSR fails, a new BSR can be automatically elected from the C-BSRs and avoid service interruption.

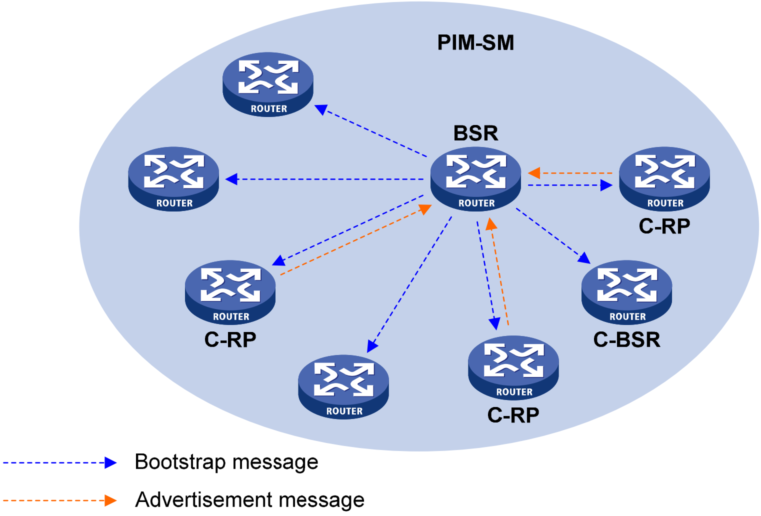
NOTE:

- An RP can provide services for multiple multicast groups, but a multicast group only uses one RP.
- A device can act as a C-RP and a C-BSR at the same time.

As shown in Figure 27, each C-RP periodically unicasts its advertisement messages (C-RP-Adv messages) to the BSR. An advertisement message contains the address of the advertising C-RP and the multicast group range to which it is designated. The BSR collects these advertisement messages and organizes the C-RP information into an RP-set, which is a database of mappings between multicast groups and RPs. The

BSR encapsulates the RP-set information in the bootstrap messages (BSMs) and floods the BSMs to the entire PIM-SM domain.

Figure 27 Information exchange between C-RPs and BSR

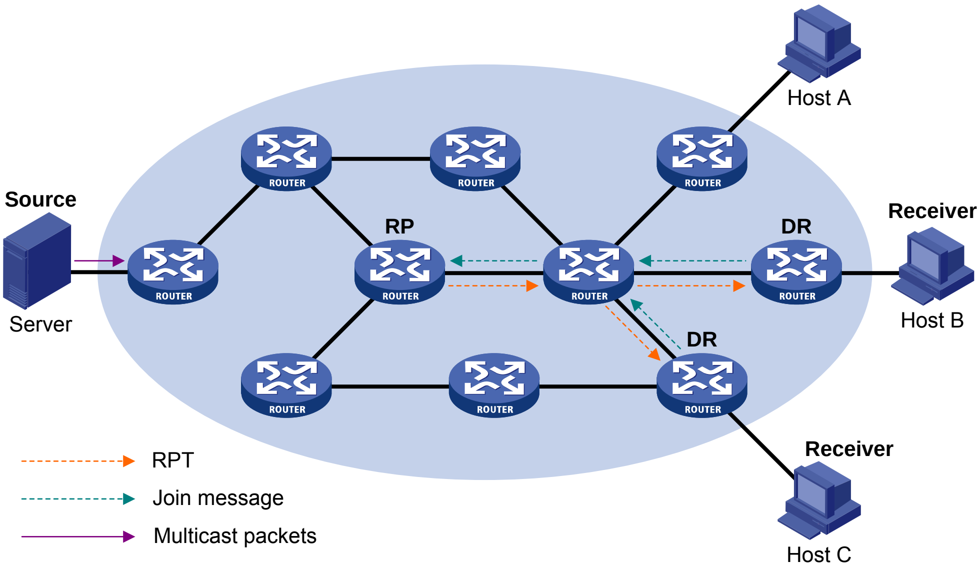


Based on the information in the RP-set, all routers in the network can select the proper RP for a specific multicast group based on the following rules:

1. The C-RP that is designated to a smaller group range wins.
2. If the group ranges are the same, the C-RP with the highest priority wins.
3. If all the C-RPs have the same priority, the C-RP with the largest hash value (calculated through the hash algorithm) wins.
4. If all the C-RPs have the same hash value, the C-RP with the highest IP address wins.

RPT building

Figure 28 RPT building in a PIM-SM domain



As shown in Figure 28, the process of building an RPT is as follows:

1. When a receiver wants to join the multicast group G, it uses an IGMP message to inform the receiver-side DR.
2. After getting the receiver information, the DR sends a join message, which is forwarded hop by hop to the RP for the multicast group.
3. The routers along the path from the DR to the RP form an RPT branch. Each router on this branch adds to its forwarding table a (*, G) entry, where the asterisk (*) means any multicast source. The RP is the root of the RPT, and the DR is a leaf of the RPT.

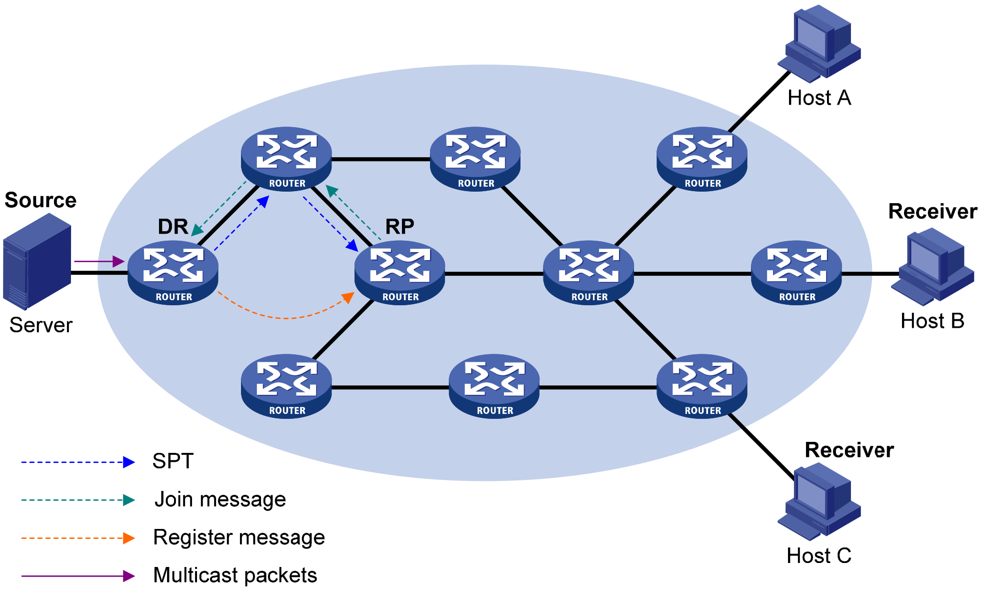
When the multicast data addressed to the multicast group G reaches the RP, the RP forwards the data to the DR along the established RPT, and finally to the receiver.

When a receiver is no longer interested in the multicast data addressed to the multicast group G, the receiver-side DR sends a prune message, which goes hop by hop along the RPT to the RP. After receiving the prune message, the upstream node deletes the interface that connects to this downstream node from the outgoing interface list and determines whether it has receivers for that multicast group. If not, the router continues to forward the prune message to its upstream router.

Multicast source registration

The multicast source uses the registration process to inform an RP of its presence.

Figure 29 Multicast source registration



As shown in Figure 29, the multicast source registers with the RP as follows:

1. The multicast source S sends the first multicast packet to the multicast group G. When receiving the multicast packet, the source-side DR encapsulates the packet in a PIM register message and unicasts the message to the RP.
2. After the RP receives the register message, it decapsulates the register message and forwards the register message down to the RPT. Meanwhile, it sends an (S, G) source-specific 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, and each router on this branch creates an (S, G) entry in its forwarding table. The source-side DR is the root of the SPT, and the RP is the leaf of the SPT.
3. The subsequent multicast data from the multicast source are forwarded to the RP along the established branch, and the RP forwards the data to the receivers along the RPT. When the

multicast data reaches the RP along the SPT, the RP unicasts a register-stop message to the source-side DR to prevent the DR from unnecessarily encapsulating the data.

Switchover to SPT

⚠ CAUTION:

If the router is an RP, disabling switchover to SPT might cause multicast traffic forwarding failures on the source-side DR. When disabling switchover to SPT, be sure you fully understand its impact on your network.

In a PIM-SM domain, only one RP and one RPT provide services for a specific multicast group. Before the switchover to SPT occurs, the source-side DR encapsulates all multicast data addressed to the multicast group in register messages and sends them to the RP. After receiving these register messages, the RP decapsulates them and forwards them to the receivers-side DR along the RPT.

Switchover to SPT has the following weaknesses:

- Encapsulation and decapsulation are complex on the source-side DR and the RP.
- The path for a multicast packet might not be the shortest one.
- The RP might be overloaded by multicast traffic bursts.

To eliminate these weaknesses, PIM-SM allows an RP or the receiver-side DR to initiate a switchover to SPT when the traffic rate exceeds a specific threshold.

- The RP initiates a switchover to SPT:

  The RP periodically checks the multicast packet forwarding rate. If the RP finds that the traffic rate exceeds the specified threshold, it sends an (S, G) source-specific 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. The subsequent multicast data for the multicast group can be forwarded to the RP along the branch without being encapsulated.

  For more information about the switchover to SPT initiated by the RP, see "Multicast source registration."

- The receiver-side DR initiates a switchover to SPT:

  The receiver-side DR periodically checks the forwarding rate for the multicast packets that the multicast source S sends to the multicast group G. If the forwarding rate exceeds the specified threshold, the DR initiates a switchover to SPT, as follows:

  a. The receiver-side DR sends an (S, G) source-specific join message hop by hop toward the multicast source. The routers along the path from the RP to the source-side DR create an (S, G) entry in their forwarding table to constitute an SPT branch.
  b. When the multicast packets for the multicast group are forwarded to the router where the RPT and the SPT branches, the router drops the multicast packets that reach it along the RPT and sends a prune message with the RP bit hop by hop to the RP. After receiving the prune message, the RP forwards it toward the multicast source (supposed only one receiver exists). Thus, the switchover to SPT is completed.
  c. Finally, the multicast source sends the multicast packets for the multicast group to the receiver along the SPT.

With the switchover to SPT, PIM-SM builds SPTs more economically than PIM-DM does.

Assert

PIM-SM uses a similar assert mechanism as PIM-DM does. For more information, see "Assert."

Administrative scoping overview

Typically, a PIM-SM domain contains only one BSR, which is responsible for advertising RP-set information within the entire PIM-SM domain. The information about all multicast groups is forwarded within the network that the BSR administers. This is called the "non-scoped BSR mechanism."

Administrative scoping mechanism

To implement refined management, you can divide a PIM-SM domain into a global-scoped zone and multiple administratively-scoped zones (admin-scoped zones). This is called the "administrative scoping mechanism."

The administrative scoping mechanism effectively releases stress on the management in a single-BSR domain and enables provision of zone-specific services through private group addresses.

Admin-scoped zones are divided for multicast groups. Zone border routers (ZBRs) form the boundary of an admin-scoped zone. Each admin-scoped zone maintains one BSR for multicast groups within a specific range. Multicast protocol packets, such as assert messages and BSMs, for a specific group range cannot cross the boundary of the admin-scoped zone for the group range. Multicast group ranges that are associated with different admin-scoped zones can have intersections. However, the multicast groups in an admin-scoped zone are valid only within the local zone, and theses multicast groups are regarded as private group addresses.

The global-scoped zone maintains a BSR for the multicast groups that do not belong to any admin-scoped zones.

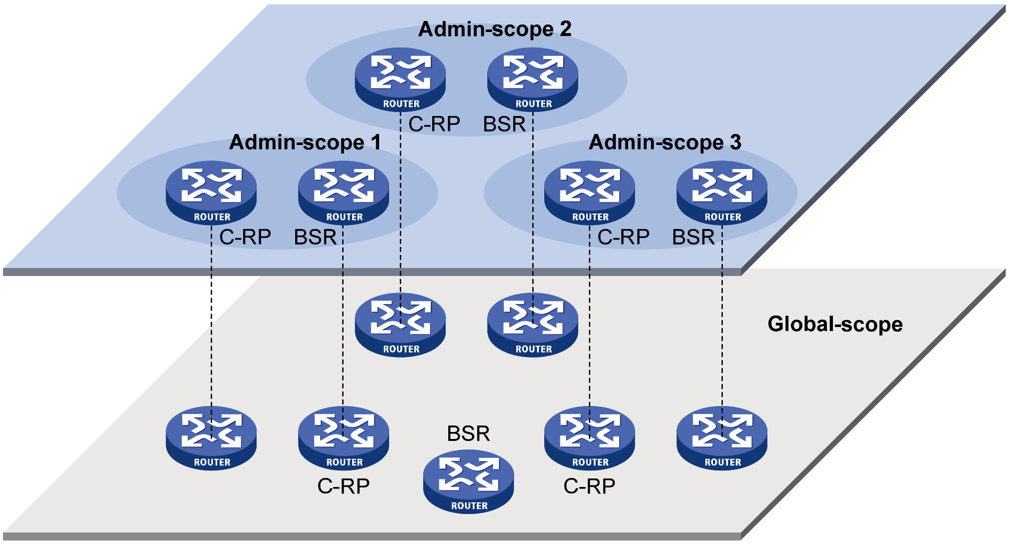
Relationship between admin-scoped zones and the global-scoped zone

The global-scoped zone and each admin-scoped zone have their own C-RPs and BSRs. These devices take effect only on their respective zones, and the BSR election and the RP election are implemented independently. Each admin-scoped zone has its own boundary. The multicast information within a zone cannot cross this boundary in either direction. You can have a better understanding of the global-scoped zone and admin-scoped zones based on geographical locations and multicast group address ranges.

- In view of geographical locations:

  An admin-scoped zone is a logical zone for particular multicast groups. The multicast packets for such multicast groups are confined within the local admin-scoped zone and cannot cross the boundary of the zone.

Figure 30 Relationship in view of geographical locations

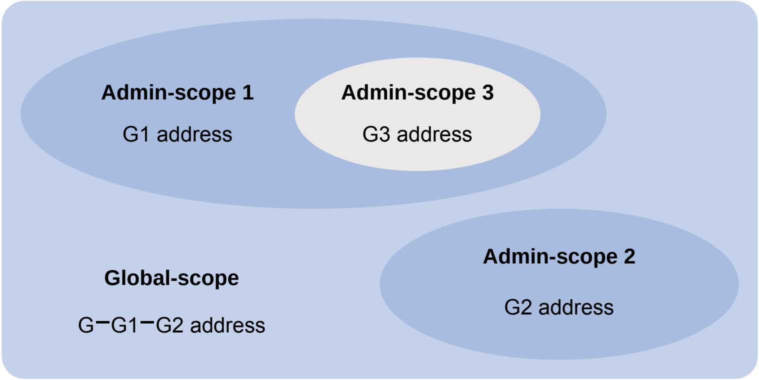


As shown in Figure 30, for the multicast groups in a specific group address range, the admin-scoped zones must be geographically separated and isolated. A router cannot belong to multiple admin-scoped zones. An admin-scoped zone contains routers that are different from other admin-scoped zones. However, the global-scoped zone includes all routers in the PIM-SM domain. Multicast packets that do not belong to any admin-scoped zones are forwarded in the entire PIM-SM domain.

- In view of multicast group address ranges:

  Each admin-scoped zone is designated to specific multicast groups, of which the multicast group addresses are valid only within the local zone. The multicast groups of different admin-scoped zones might have intersections. All the multicast groups other than those of the admin-scoped zones use the global-scoped zone.

Figure 31 Relationship in view of multicast group address ranges



As shown in Figure 31, the admin-scoped zones 1 and 2 have no intersection, but the admin-scoped zone 3 is a subset of the admin-scoped zone 1. The global-scoped zone provides services for all the multicast groups that are not covered by the admin-scoped zones 1 and 2, G–G1–G2 in this case.

PIM-SSM overview

The ASM model includes PIM-DM and PIM-SM. The SSM model can be implemented by leveraging part of the PIM-SM technique. It is also called "PIM-SSM."

The SSM model provides a solution for source-specific multicast. It maintains the relationship between hosts and routers through IGMPv3.

In actual applications, part of IGMPv3 and PIM-SM techniques are adopted to implement the SSM model. In the SSM model, because receivers have located a multicast source, no RP or RPT is required, multicast sources do not register, and the MSDP is not needed for discovering multicast sources in other PIM domains.

The operating mechanism of PIM-SSM is summarized as follows:

- Neighbor discovery
- DR election
- SPT building

Neighbor discovery

PIM-SSM uses the same neighbor discovery mechanism as PIM-SM. For more information, see "Neighbor discovery."

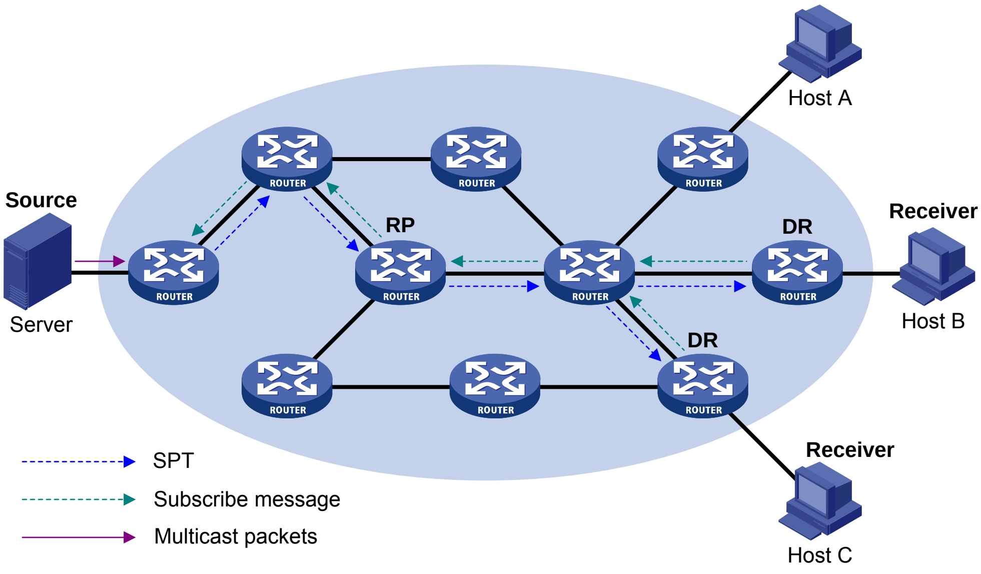
DR election

PIM-SSM uses the same DR election mechanism as PIM-SM. For more information, see "DR election."

SPT building

The decision to build an RPT for PIM-SM or an SPT for PIM-SSM depends on whether the multicast group that the receiver wants to join is included in the SSM group range (232.0.0.0/8 reserved by IANA).

Figure 32 SPT building in PIM-SSM



As shown in Figure 32, Host B and Host C are receivers. They send IGMPv3 report messages to their DRs to express their interest in the multicast information that the multicast source S sends to the multicast group G.

After receiving a report message, the DR first checks whether the group address in this message is in the SSM group range and does the following:

- If the group address is in the SSM group range, the DR sends a subscribe message hop by hop toward the multicast source S. All routers along the path from the DR to the source create an (S, G) entry so as to build an SPT, which is rooted at the multicast source S and has the receivers as its leaves. This SPT is the transmission channel in PIM-SSM.
- If the group address is not in the SSM group range, the receiver-side DR sends a (*, G) join message to the RP, and the multicast source registers with the source-side DR.

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

PIM support for VPNs

To support PIM for VPNs, a multicast router that runs PIM maintains an independent set of PIM neighbor table, multicast routing table, BSR information, and RP-set information for each VPN.

After receiving a multicast data packet, the multicast router checks which VPN the data packet belongs to, and then forwards the packet according to the multicast routing table for that VPN or creates a multicast routing entry for that VPN.

Protocols and standards

- RFC 3973, *Protocol Independent Multicast-Dense Mode (PIM-DM): Protocol Specification(Revised)*
- RFC 4601, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)*
- RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*
- RFC 4607, *Source-Specific Multicast for IP*
- Draft-ietf-ssm-overview-05, *An Overview of Source-Specific Multicast (SSM)*

Configuring PIM-DM

PIM-DM configuration task list

Task at a glance
(Required.) Enabling PIM-DM
(Optional.) Enabling the state refresh feature
(Optional.) Configuring state refresh parameters
(Optional.) Configuring PIM-DM graft retry timer
(Optional.) Configuring common PIM features

Configuration prerequisites

Before you configure PIM-DM, configure a unicast routing protocol so that all devices in the domain are interoperable at the network layer

Enabling PIM-DM

Enable IP multicast routing before you configure PIM.

With PIM-DM enabled on interfaces, routers can establish PIM neighbor relationship and process PIM messages from their PIM neighbors. When you deploy a PIM-DM domain, enable PIM-DM on all non-border interfaces of the routers.

IMPORTANT:

All the interfaces on a device must operate in the same PIM mode in the public network or the same VPN instance.

To enable PIM-DM:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable IP multicast routing and enter MRIB view.	**multicast routing** [**vpn-instance** *vpn-instance-name*]	By default, IP multicast routing is disabled.
3.	Return to system view.	**quit**	N/A
4.	Enter interface view.	**interface** *interface-type interface-number*	N/A
5.	Enable PIM-DM.	**pim dm**	By default, PIM-DM is disabled.

Enabling the state refresh feature

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 shared-media subnet can have the state refresh feature only if the state refresh feature is enabled on all PIM routers on the subnet.

To enable the state refresh feature on all routers in PIM-DM domain:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter interface view.	**interface** *interface-type interface-number*	N/A
3.	Enable the state refresh feature.	**pim state-refresh-capable**	By default, the state refresh feature is enabled.

Configuring state refresh parameters

The router directly connected with the multicast source periodically sends state refresh messages. You can configure the interval for sending such messages on that router.

A router might receive duplicate state refresh messages within a short time. To prevent this situation, you can configure the amount of time that the router must wait before it receives next state refresh message.

If the router receives a new state refresh message within the specified waiting time, it discards the message. If this timer times out, the router accepts a new state refresh message, refreshes its own PIM-DM state, and resets the waiting timer.

The TTL value of a state refresh message decrements by 1 whenever it passes a router before it is forwarded to the downstream node until the TTL value comes down to 0. In a small network, a state refresh message might cycle in the network. To effectively control the propagation scope of state refresh messages, configure an appropriate TTL value based on the network size on the router directly connected with the multicast source.

To configure state refresh parameters:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	N/A
3. Configure the interval to send state refresh messages.	**state-refresh-interval** *interval*	By default, the interval to send state refresh messages is 60 seconds.
4. Configure the time to wait before receiving a new state refresh message.	**state-refresh-rate-limit** *time*	By default, the waiting time is 30 seconds.
5. Configure the TTL value of state refresh messages.	**state-refresh-ttl** *ttl-value*	By default, the TTL value of state refresh messages is 255.

Configuring PIM-DM graft retry timer

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 known as graft retry timer, until it receives a graft-ack message from the upstream router. For more information about the configuration of other timers in PIM-DM, see "Configuring common PIM timers."

To configure the graft retry timer:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the graft retry timer.	**pim timer graft-retry** *interval*	By default, the graft retry timer is 3 seconds.

Configuring PIM-SM

PIM-SM configuration task list

Task at a glance
(Required.) Enabling PIM-SM
(Required.) Configuring an RP • Configuring a static RP • Configuring a C-RP NOTE: Perform at least one of the above tasks. In a network with a static RP, skip the task of configuring a BSR.
Configuring a BSR: • (Required.) Configuring a C-BSR • (Optional.) Configuring a PIM domain border • (Optional.) Disabling the BSM semantic fragmentation function
(Optional.) Configuring multicast source registration
(Optional.) Configuring switchover to SPT
(Optional.) Configuring common PIM features

Configuration prerequisites

Before you configure PIM-SM, configure a unicast routing protocol so that all devices in the domain are interoperable at the network layer.

Enabling PIM-SM

Enable IP multicast routing before you configure PIM.

With PIM-SM enabled on interfaces, routers can establish PIM neighbor relationship and process PIM messages from their PIM neighbors. When you deploy a PIM-SM domain, HP recommends that you enable PIM-SM on all non-border interfaces.

IMPORTANT:

All the interfaces on the same router must operate in the same PIM mode in the public network or the same VPN instance.

To enable PIM-SM:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable IP multicast routing and enter MRIB view.	**multicast routing** [**vpn-instance** *vpn-instance-name*]	By default, IP multicast routing is disabled.

Step		Command	Remarks
3.	Return to system view.	**quit**	N/A
4.	Enter interface view.	**interface** *interface-type interface-number*	N/A
5.	Enable PIM-SM.	**pim sm**	By default, PIM-SM is disabled.

Configuring an RP

An RP can provide services for multiple or all multicast groups. However, only one RP can forward multicast traffic for a multicast group at a moment.

An RP can be manually configured or dynamically elected through the BSR mechanism. For a large-scaled PIM network, configuring static RPs is a tedious job. Generally, static RPs are backups for dynamic RPs to enhance the robustness and operational manageability on a multicast network.

Configuring a static RP

If only one dynamic RP exists on a network, you can configure a static RP to avoid communication interruption caused by single-point failures. It can also avoid waste of bandwidth due to frequent message exchange between C-RPs and the BSR. The static RP configuration must be the same on all routers in the PIM-SM domain.

To configure a static RP:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure a static RP for PIM-SM.	**static-rp** *rp-address* [*acl-number* | **preferred**] *	By default, no static RP is configured.

Configuring a C-RP

IMPORTANT:

When you configure a C-RP, reserve a relatively large bandwidth between the C-RP and the other devices in the PIM-SM domain.

In a PIM-SM domain, if you want a router to become the RP, you can configure the router as a C-RP. The BSR collects the C-RP information according to the received advertisement messages from C-RPs or the auto-RP announcements from other routers. Then, it organizes the C-RP information into the RP-set information, which is flooded throughout the entire network. Then, the other routers in the network can determine the RPs for different multicast group ranges based on the RP-set information. HP recommends configuring C-RPs on backbone routers.

To enable the BSR to distribute the RP-set information in the PIM-SM domain, the C-RPs must periodically send advertisement messages to the BSR. The BSR learns the C-RP information, encapsulates the C-RP information and its own IP address in a BSM, and floods the BSM to all PIM routers in the domain.

An advertisement message contains a holdtime option, which defines the C-RP lifetime for the advertising C-RP. After the BSR receives an advertisement message from a C-RP, it starts a timer for the C-RP. If the BSR does not receive any advertisement message when the timer expires, it regards the C-RP failed or unreachable.

To guard against C-RP spoofing, you must configure a legal C-RP address range and the multicast group range to which the C-RP is designated. In addition, because every C-BSR might become the BSR, you must configure the same filtering policy on all C-BSRs in the PIM-SM domain.

To configure a C-RP:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	N/A
3. Configure a C-RP.	**c-rp** *ip-address* [**advertisement-interval** *adv-interval* | **group-policy** *acl-number* | **holdtime** *hold-time* | **priority** *priority*] *	By default, no C-RP is configured.
4. (Optional.) Configure a legal C-RP address range and the multicast group range to which the C-RP is designated.	**crp-policy** *acl-number*	By default, no restrictions are defined.

Configuring a BSR

You must configure a BSR if C-RPs are configured to dynamically select the RP. In a network with a static RP, this configuration task is unnecessary.

A PIM-SM domain can have only one BSR, but must have at least one C-BSR. Any router can be configured as a C-BSR. Elected from C-BSRs, the BSR is responsible for collecting and advertising RP information in the PIM-SM domain.

Configuring a C-BSR

C-BSRs should be configured on routers on the backbone network. The BSR election process is summarized as follows:

- Initially, each C-BSR regards itself as the BSR of the PIM-SM domain and sends BSMs to other routers in the domain.
- When a C-BSR receives the BSM from another C-BSR, it compares its own priority with the priority carried in the message. The C-BSR with a higher priority wins the BSR election. If a tie exists in the priority, the C-BSR with a higher IP address wins. The loser uses the winner's BSR address to replace its own BSR address and no longer regards itself as the BSR, and the winner retains its own BSR address and continues to regard itself as the BSR.

In a PIM-SM domain, the BSR collects C-RP information from the received advertisement messages from the C-RPs, encapsulates the C-RP information in the RP-set information, and distributes the RP-set information to all routers in the PIM-SM domain. All routers use the same hash algorithm to get an RP for a specific multicast group.

Configuring a legal BSR address range enables filtering of BSMs based on the address range, thereby preventing a maliciously configured host from masquerading as a BSR. The same configuration must be made on all routers in the PIM-SM domain. The following describes the typical BSR spoofing cases and the corresponding preventive measures:

- Some maliciously configured hosts can forge BSMs to fool routers and change RP mappings. Such attacks often occur on border routers. Because a BSR is inside the network whereas hosts are outside the network, you can protect a BSR against attacks from external hosts by enabling the border routers to perform neighbor checks and RPF checks on BSMs and to discard unwanted messages.
- When an attacker controls a router in the network or when an illegal router is present in the network, the attacker can configure the router as a C-BSR and make it win the BSR election to advertise RP information in the network. After a router is configured as a C-BSR, it automatically floods the network with BSMs. Because a BSM has a TTL value of 1, the whole network will not be affected as long as the neighbor router discards these BSMs. Therefore, with a legal BSR address range configured on all routers in the network, all these routers can discard BSMs from out of the legal address range.

These preventive measures can partially protect the BSR in a network. However, if an attacker controls a legal BSR, the problem still exists.

When you configure a C-BSR, reserve a relatively large bandwidth between the C-BSR and the other devices in the PIM-SM domain.

When C-BSRs connect to other PIM routers through tunnels, static multicast routes must be configured to make sure the next hop to a C-BSR is a tunnel interface. Otherwise, RPF check is affected. For more information about static multicast routes, see "Configuring multicast routing and forwarding."

To configure a C-BSR:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure a C-BSR.	**c-bsr** *ip-address* [**scope** *group-address* { *mask-length* | *mask* }] [**hash-length** *hash-length* | **priority** *priority*] *	By default, no C-BSR is configured.
4.	(Optional.) Configure a legal BSR address range.	**bsr-policy** *acl-number*	By default, no restrictions are defined.

Configuring a PIM domain border

As the administrative core of a PIM-SM domain, the BSR sends the collected RP-set information in the form of bootstrap messages to all routers in the PIM-SM domain.

A PIM domain border is a bootstrap message boundary. Each BSR has its specific service scope. A number of PIM domain border interfaces partition a network into different PIM-SM domains. Bootstrap messages cannot cross a domain border in either direction.

Perform the following configuration on routers that you want to configure as a PIM domain border.

To configure a PIM domain border:

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

Step	Command	Remarks
3. Configure a PIM domain border.	**pim bsr-boundary**	By default, no PIM domain border is configured.

Disabling the BSM semantic fragmentation function

Generally, a BSR periodically advertises the RP-set information in BSMs within the PIM-SM domain. It encapsulates a BSM in an IP datagram and might fragment the datagram if the message exceeds the MTU. In this case, 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 BSM fragments (BSMFs).

- If the RP-set information for a multicast group range is carried in one BSMF, a non-BSR router directly updates the RP-set information for the group range after receiving the BSMF.
- If the RP-set information for a multicast group range is carried in multiple BSMFs, a non-BSR router updates the RP-set information for the group range after receiving all these BSMFs. Because the RP-set information contained in each segment is different, loss of some IP fragments does not result in dropping of the entire BSM.

The BSM semantic fragmentation function is enabled by default. A device that does not support this function might regard a fragment as a BSM and thus learns only part of the RP-set information. Therefore, if such devices exist in the PIM-SM domain, you must disable the BSM semantic fragmentation function on the C-BSRs.

To disable the BSM semantic fragmentation function:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	N/A
3. Disable the BSM semantic fragmentation function.	**undo bsm-fragment enable**	By default, BSM semantic fragmentation is enabled.

NOTE:

Generally, a BSR performs BSM semantic fragmentation according to the MTU of its BSR interface. However, for BSMs originated due to learning of a new PIM neighbor, semantic fragmentation is performed according to the MTU of the interface that sends the BSMs.

Configuring multicast source registration

In a PIM-SM domain, the source-side DR sends register messages to the RP, and these register messages have different multicast source or group addresses. You can configure a filtering rule to filter register messages so that the RP can provide services for specific multicast groups. If the filtering rule denies an (S, G) entry, or if the filtering rule does not define the action for this entry, the RP sends a register-stop message to the DR to stop the registration process for the multicast data.

In view of information integrity of a register message in the transmission process, you can configure the device to calculate the checksum based on the entire register message. However, to reduce the workload of encapsulating data in register messages and for the sake of interoperability, do not use this checksum calculation method.

To configure multicast source registration:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure a filtering rule for register messages.	**register-policy** *acl-number*	By default, no register filtering rule exists.
4.	Configure the device to calculate the checksum based on the entire register message.	**register-whole-checksum**	By default, the device calculates the checksum based on the header of a register message.

Configuring switchover to SPT

CAUTION:

If the router is an RP, disabling switchover to SPT might cause multicast traffic forwarding failures on the source-side DR. When disabling switchover to SPT, be sure you fully understand its impact on your network.

Both the receiver-side DR and RP can monitor the traffic rate of passing-by multicast packets and thus trigger a switchover from RPT to SPT.

To configure the switchover to SPT:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure the criteria for triggering a switchover to SPT.	**spt-switch-threshold** { *traffic-rate* | **immediacy** | **infinity** } [**group-policy** *acl-number*]	By default, the device immediately triggers a switchover to SPT after receiving the first multicast packet.

NOTE:

If the multicast source information is learned through MSDP, the device switches to SPT immediately after it receives the first multicast packet, regardless of the traffic rate threshold.

Configuring PIM-SSM

PIM-SSM requires IGMPv3 support. Enable IGMPv3 on PIM routers that connect to multicast receivers.

PIM-SSM configuration task list

Task	Remarks
Enabling PIM-SM	Required.
Configuring the SSM group range	Optional.
Configuring common PIM features	Optional.

Configuration prerequisites

Before you configure PIM-SSM, configure a unicast routing protocol so that all devices in the domain are interoperable at the network layer.

Enabling PIM-SM

The implementation of the SSM model is based on subsets of PIM-SM. Therefore, you must enable PIM-SM before configuring PIM-SSM.

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

IMPORTANT:

All the interfaces on a device must be enabled with the same PIM mode.

To enable PIM-SM:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable IP multicast routing, and enter MRIB view.	**multicast routing** [**vpn-instance** *vpn-instance-name*]	By default, IP multicast routing is disabled.
3.	Return to system view.	**quit**	N/A
4.	Enter interface view.	**interface** *interface-type interface-number*	N/A
5.	Enable PIM-SM.	**pim sm**	By default, PIM-SM is disabled.

Configuring the SSM group range

When a PIM-SM enabled interface receives a multicast packet, it checks whether the multicast group address of the packet is in the SSM group range. If the multicast group address is in this range, the PIM mode for this packet is PIM-SSM. If the multicast group address is not in this range, the PIM mode is PIM-SM.

Configuration guidelines

- Perform the following configuration on all routers in the PIM-SSM domain.
- Make sure the same SSM group range is configured on all routers in the entire domain. Otherwise, multicast information cannot be delivered through the SSM model.

- When a member of a multicast group in the SSM group range sends an IGMPv1 or IGMPv2 report message, the device does not trigger a (*, G) join.

Configuration procedure

To configure an SSM group range:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter PIM view.	**pim**	N/A
3.	Configure the SSM group range.	**ssm-policy** *acl-number*	The default range is 232.0.0.0/8.

Configuring common PIM features

Configuration task list

Task at a glance
(Optional.) Configuring a multicast data filter
(Optional.) Configuring a hello message filter
(Optional.) Configuring PIM hello message options
(Optional.) Configuring common PIM timers
(Optional.) Setting the maximum size of each join or prune message
(Optional.) Enabling PIM to work with BFD

Configuration prerequisites

Before you configure common PIM features, complete the following tasks:

- Configure a unicast routing protocol so that all devices in the domain are interoperable at the network layer.
- Configure PIM-DM, or PIM-SM.

Configuring a multicast data filter

In either a PIM-DM domain or a PIM-SM domain, routers can check passing-by multicast data and determine whether to continue forwarding the multicast data based on the configured filtering rules. You can configure a PIM router to act as a multicast data filter to help implement traffic control and control the information available to downstream receivers.

A filter can filter not only independent multicast data but also multicast data encapsulated in register messages. Generally, a filter nearer to the multicast source has a better filtering effect.

To configure a multicast data filter:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure a multicast data filter:	**source-policy** *acl-number*	By default, no multicast data filter is configured.

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.

To guard against PIM message attacks, you can configure a legal source address range for hello messages on interfaces of routers to ensure the correct PIM neighboring relationships.

To configure a hello message filter:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure a hello message filter.	**pim neighbor-policy** *acl-number*	By default, no hello message filter exists. If a PIM neighbor's hello messages cannot pass the filter, the neighbor is automatically removed when its maximum number of hello attempts is reached.

Configuring PIM hello message options

In either a PIM-DM domain or a PIM-SM domain, hello messages exchanged among routers contain the following configurable options:

- **DR_Priority** (for PIM-SM only)—Priority for DR election. The device with the highest priority wins the DR election. You can configure this option for all the routers in a shared-media LAN that directly connects to the multicast source or the receivers.
- **Holdtime**—PIM neighbor lifetime. If a router does not receive a hello message from a neighbor when the neighbor lifetime expires, it regards the neighbor failed or unreachable.
- **LAN_Prune_Delay**—Delay of forwarding prune messages on a shared-media LAN. This option consists of LAN delay (namely, prune message delay), override interval, and neighbor tracking support (namely, the capability to disable join message suppression).

  The prune message delay defines the delay time for a router to forward a received prune message to the upstream routers. The override interval defines a period for a downstream router to override a prune message. If the prune message delay or override interval on different PIM routers on a shared-media LAN are different, the largest value takes effect.

A router does not immediately prune an interface after it receives a prune message from the interface. Instead, it starts a timer (the prune message delay plus the override interval). If interface receives a join message before the override interval expires, the router does not prune the interface. Otherwise, the router prunes the interface when the timer (the prune message delay plus the override interval) expires.

You can enable the neighbor tracking function (or disable the join message suppression function) on an upstream router to track the states of the downstream nodes that have sent the join message and the joined state holdtime timer has not expired. If you want to enable the neighbor tracking function, you must enable it on all PIM routers on a shared-media LAN. Otherwise, the upstream router cannot track join messages from every downstream routers.

- **Generation ID**—A router generates a generation ID for hello messages when an interface is enabled with PIM. The generation ID is a random value, but only changes when the status of the router changes. 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 router has changed. In this case, it sends a join message to the upstream router for status update. You can configure an interface to drop hello messages without the generation ID options to promptly know the status of an upstream router.

You can configure hello message options in PIM view or interface view. The configurations made in PIM view take effect on all interfaces and the configurations made in interface view take effect only on the current interface. If you configure hello message options in both PIM view and interface view, the configuration in interface view always takes precedence.

Configuring hello message options globally

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	N/A
3. Set the DR priority.	**hello-option dr-priority** *priority*	By default, the DR priority is 1.
4. Set the neighbor lifetime.	**hello-option holdtime** *time*	By default, the neighbor lifetime is 105 seconds.
5. Set the prune message delay.	**hello-option lan-delay** *delay*	By default, the prune message delay is 500 milliseconds.
6. Set the override interval.	**hello-option override-interval** *interval*	By default, the override interval is 2500 milliseconds.
7. Enable the neighbor tracking function.	**hello-option neighbor-tracking**	By default, the neighbor tracking function is disabled.

Configuring hello message options on an interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Set the DR priority.	**pim hello-option dr-priority** *priority*	By default, the DR priority is 1.
4. Set the neighbor lifetime.	**pim hello-option holdtime** *time*	By default, the neighbor lifetime is 105 seconds.

Step		Command	Remarks
5.	Set the prune delay.	**pim hello-option lan-delay** *delay*	By default, the prune delay is 500 milliseconds.
6.	Set the override interval.	**pim hello-option override-interval** *interval*	By default, the override interval is 2500 milliseconds.
7.	Enable the neighbor tracking function.	**pim hello-option neighbor-tracking**	By default, the neighbor tracking function is disabled.
8.	Enable dropping hello messages without the Generation ID option.	**pim require-genid**	By default, an interface accepts hello messages without the Generation ID option.

Configuring common PIM timers

PIM routers periodically send hello messages to discover PIM neighbors, and maintain PIM neighbor relationship.

After receiving a hello message, a PIM router waits for a random time period before sending a hello message. This random time period is smaller than the maximum delay for sending hello messages, and it can avoid collisions that might occur when multiple PIM routers send hello messages simultaneously.

A PIM router periodically sends join/prune messages to its upstream routers for state update. A join/prune message contains the joined/pruned state holdtime value, and an upstream router uses this value to set a holdtime timer for the joined state or pruned state of the downstream interfaces.

When a router fails to receive subsequent multicast data from the multicast source S, the router does not immediately remove the corresponding (S, G) entry. Instead, it maintains the (S, G) entry for a period of time (known as, the multicast source lifetime) before deleting the (S, G) entry.

You can configure common PIM timers in PIM view or interface view. The configurations made in PIM view take effect on all interfaces. The configurations made in interface view take effect only on the current interface. If you configure common PIM timers in both PIM view and interface view, the configuration in interface view always takes precedence.

TIP:

For a network without special requirements, HP recommends using the defaults.

Configuring common PIM timers globally

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Set the interval to send hello messages.	**timer hello** *interval*	By default, the interval to send hello messages is 30 seconds.
4.	Set the interval to send join/prune messages.	**timer join-prune** *interval*	By default, the interval to send join/prune messages is 60 seconds.
5.	Set the joined/pruned state holdtime timer.	**holdtime join-prune** *time*	By default, the joined/pruned state holdtime timer is 210 seconds.

Step	Command	Remarks
6. Set the multicast source lifetime.	**source-lifetime** *time*	By default, the multicast source lifetime is 210 seconds.

Configuring common PIM timers on an interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Set the interval to send hello messages.	**pim timer hello** *interval*	By default, the interval to send hello messages is 30 seconds.
4. Set the maximum delay for sending a hello message.	**pim triggered-hello-delay** *delay*	By default, the maximum delay for sending a hello message is 5 seconds.
5. Set the interval to send join/prune messages.	**pim timer join-prune** *interval*	By default, the interval to send join/prune messages is 60 seconds.
6. Set the joined/pruned state holdtime timer.	**pim holdtime join-prune** *time*	By default, the joined/pruned state holdtime timer is 210 seconds.

Setting the maximum size of each join or prune message

The loss of an oversized join or prune message might result in loss of massive information. You can set a small value for the size of each join or prune message to reduce the impact.

To set the maximum size of each join or prune message:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter PIM view.	**pim** [**vpn-instance** *vpn-instance-name*]	N/A
3. Set the maximum size of each join or prune message.	**jp-pkt-size** *size*	By default, the maximum size of a join or prune message is 8100 bytes.

Enabling PIM to work with BFD

PIM uses hello messages to elect a DR for a shared-media network. The elected DR is the only multicast forwarder on the shared-media network.

If the DR fails, a new DR election process will start after the DR ages out. However, it might take a long period of time before other routers detect the link failures and trigger a new DR election. To start a new DR election process immediately after the original DR fails, enable PIM to work with BFD on a shared-media 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 shared-media network, so that the PIM neighbors can fast detect DR failures and start a new DR election process. For more information about BFD, see *High Availability Configuration Guide*.

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

To enable PIM to work with BFD:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter interface view.	**interface** *interface-type interface-number*	N/A
3.	Enable PIM to work with BFD.	**pim bfd enable**	By default, PIM is disabled to work with BFD.

Displaying and maintaining PIM

Execute **display** commands in any view.

Task	Command
Display BSR information in the PIM-SM domain.	**display pim** [**vpn-instance** *vpn-instance-name*] **bsr-info**
Display information about the routes used by PIM.	**display pim** [**vpn-instance** *vpn-instance-name*] **claimed-route** [*source-address*]
Display C-RP information in the PIM-SM domain.	**display pim** [**vpn-instance** *vpn-instance-name*] **c-rp** [**local**]
Display PIM information on an interface.	**display pim** [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**]
Display PIM neighbor information.	**display pim** [**vpn-instance** *vpn-instance-name*] **neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *
Display PIM routing table information.	**display pim** [**vpn-instance** *vpn-instance-name*] **routing-table** [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **flags** *flag-value* | **fsm** | **incoming-interface** *interface-type interface-number* | **mode** *mode-type* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *
Display RP information in the PIM-SM domain.	**display pim** [**vpn-instance** *vpn-instance-name*] **rp-info** [*group-address*]
Display statistics for PIM packets.	**display pim statistics**

PIM configuration examples

PIM-DM configuration example

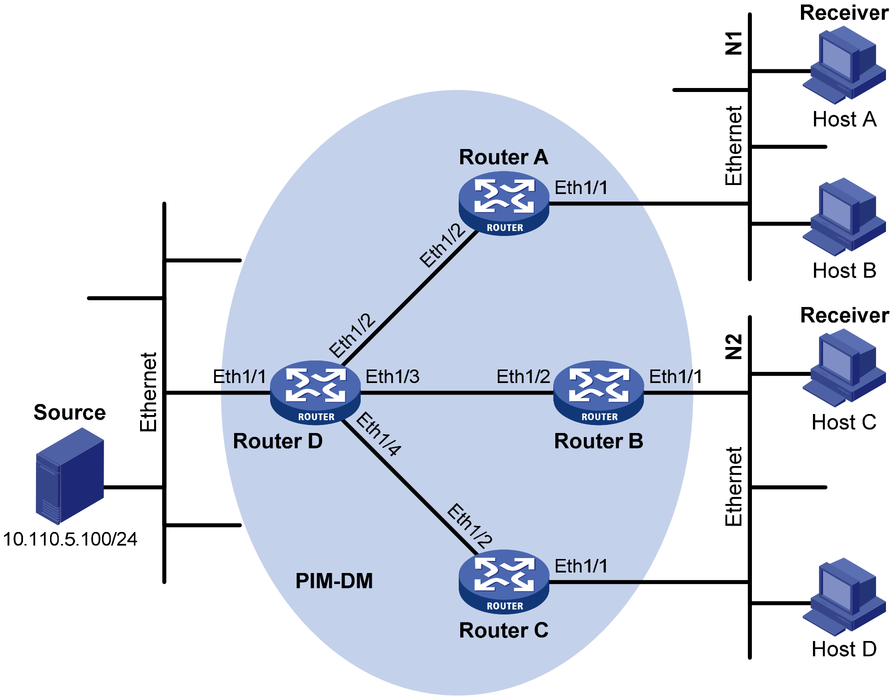
Network requirements

As shown in Figure 33, VOD streams are sent to receiver hosts in 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 N1 and N2.

IGMPv2 runs between Router A and N1 and between Router B, Router C, and N2.

Figure 33 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Router A	Eth1/1	10.110.1.1/24	Router D	Eth1/1	10.110.5.1/24
	Eth1/2	192.168.1.1/24		Eth1/2	192.168.1.2/24
Router B	Eth1/1	10.110.2.1/24		Eth1/3	192.168.2.2/24
	Eth1/2	192.168.2.1/24		Eth1/4	192.168.3.2/24
Router C	Eth1/1	10.110.2.2/24			
	Eth1/2	192.168.3.1/24			

Configuration procedure

1. Configure the IP address and subnet mask for each interface as per Figure 33. (Details not shown.)
2. Configure OSPF on the routers in the PIM-DM domain to make sure network-layer is interoperable among the routers and routing information among the routers can be dynamically updated. (Details not shown.)
3. Enable IP multicast routing, IGMP, and PIM-DM :

# On Router A, enable IP multicast routing globally, enable IGMP on Ethernet 1/1, and enable PIM-DM on each interface.

```
<RouterA> system-view
[RouterA] multicast routing
[RouterA-mrib] quit
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] igmp enable
[RouterA-Ethernet1/1] pim dm
[RouterA-Ethernet1/1] quit
[RouterA] interface ethernet 1/2
[RouterA-Ethernet1/2] pim dm
[RouterA-Ethernet1/2] quit
```

# Enable IP multicast routing, IGMP, and PIM-DM on Router B and Router C in the same way Router A is configured. (Details not shown.)

# On Router D, enable IP multicast routing globally, and enable PIM-DM on each interface.

```
<RouterD> system-view
[RouterD] multicast routing
[RouterD-mrib] quit
[RouterD] interface ethernet 1/1
[RouterD-Ethernet1/1] pim dm
[RouterD-Ethernet1/1] quit
[RouterD] interface ethernet 1/2
[RouterD-Ethernet1/2] pim dm
[RouterD-Ethernet1/2] quit
[RouterD] interface ethernet 1/3
[RouterD-Ethernet1/3] pim dm
[RouterD-Ethernet1/3] quit
[RouterD] interface ethernet 1/4
[RouterD-Ethernet1/4] pim dm
[RouterD-Ethernet1/4] quit
```

Verifying the configuration

# Display PIM information on Router D.

```
[RouterD] display pim interface
 Interface           NbrCnt HelloInt   DR-Pri     DR-Address
 Eth1/1              0      30         1          10.110.5.1     (local)
 Eth1/2              1      30         1          192.168.1.2    (local)
 Eth1/3              1      30         1          192.168.2.2    (local)
 Eth1/4              1      30         1          192.168.3.2    (local)
```

# Display the PIM neighboring relationships on Router D.

```
[RouterD] display pim neighbor
 Total Number of Neighbors = 3

 Neighbor         Interface           Uptime   Expires  Dr-Priority
 192.168.1.1      Eth1/2              00:02:22 00:01:27 1
 192.168.2.1      Eth1/3              00:00:22 00:01:29 3
 192.168.3.1      Eth1/4              00:00:23 00:01:31 5
```

Assume that Host A needs to receive the information addressed to multicast group 225.1.1.1. After the multicast source 10.110.5.100/24 sends multicast packets to the multicast group, an SPT is established through traffic flooding. Routers on the SPT path (Router A and Router D) have their (S, G) entries. Host A sends an IGMP report to Router A to join the multicast group G, and a (*, G) entry is generated on Router A. You can use the **display pim routing-table** command to display the PIM routing table information on each router. For example:

# Display the PIM routing table information on Router A.

```
[RouterA] display pim routing-table
 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: Ethernet1/1
             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: Ethernet1/2
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Ethernet1/1
             Protocol: pim-dm, UpTime: 00:04:25, Expires: never
```

# Display the PIM routing table information on Router D.

```
[RouterD] display pim routing-table
 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: Ethernet1/1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 2
         1: Ethernet1/2
             Protocol: pim-dm, UpTime: 00:03:27, Expires: never
         2: Ethernet1/4
             Protocol: pim-dm, UpTime: 00:03:27, Expires: never
```

PIM-SM non-scoped zone configuration example

Network requirements

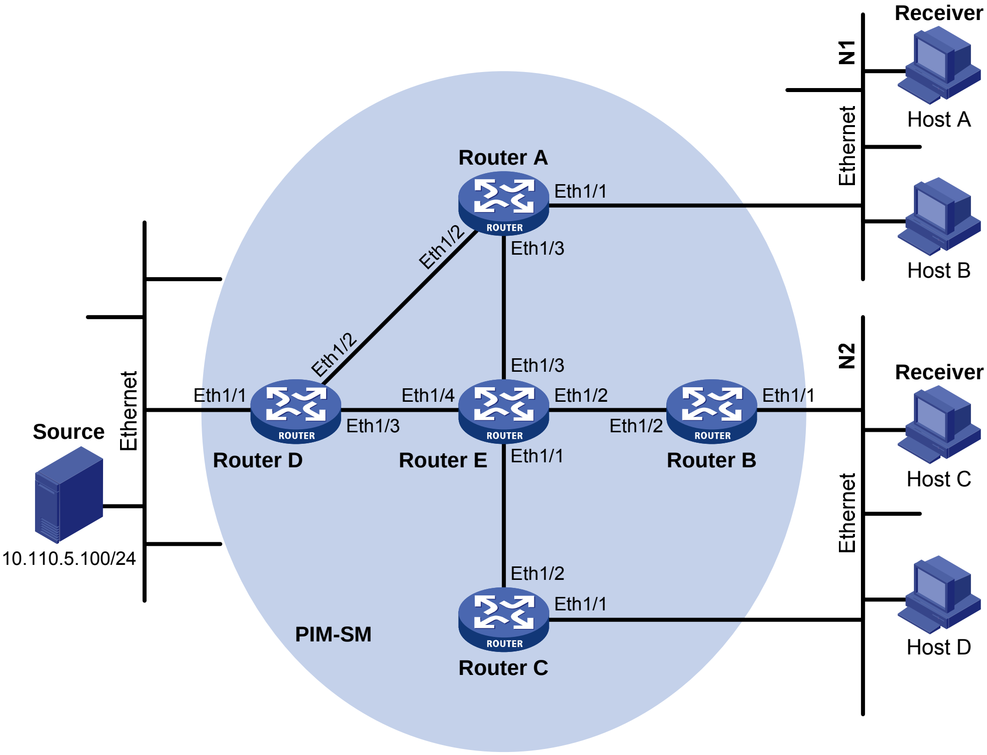
As shown in Figure 34, VOD streams are sent to receiver hosts in multicast. The receivers of different subnets form stub networks, and at least one receiver host exist in each stub network. The entire PIM-SM domain contains only one BSR.

Host A and Host C are multicast receivers in the stub networks N1 and N2.

Ethernet 1/3 on Router D and Ethernet 1/3 on Router E act as C-BSRs and C-RPs. The C-BSR on Router E has a higher priority. The C-RPs are designated to the multicast group range 225.1.1.0/24. Modify the hash mask length to map the multicast group range to the two C-RPs.

IGMPv2 runs between Router A and N1, and between Router B, Router C, and N2.

Figure 34 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Router A	Eth1/1	10.110.1.1/24	Router D	Eth1/1	10.110.5.1/24
	Eth1/2	192.168.1.1/24		Eth1/2	192.168.1.2/24
	Eth1/3	192.168.9.1/24		Eth1/3	192.168.4.2/24
Router B	Eth1/1	10.110.2.1/24	Router E	Eth1/1	192.168.3.2/24
	Eth1/2	192.168.2.1/24		Eth1/2	192.168.2.2/24
Router C	Eth1/1	10.110.2.2/24		Eth1/3	192.168.9.2/24
	Eth1/2	192.168.3.1/24		Eth1/4	192.168.4.1/24

Configuration procedure

1. Assign an IP address and subnet mask to each interface according to Figure 34. (Details not shown.)

2. Enable OSPF on all routers on the PIM-SM network to make sure the network-layer on the PIM-SM network is interoperable and the routing information among the routers can be dynamically updated. (Details not shown.)
3. Enable IP multicast routing, IGMP and PIM-SM:

   # On Router A, enable IP multicast routing globally, enable IGMP on Ethernet 1/1, and enable PIM-SM on each interface.

   ```
   <RouterA> system-view
   [RouterA] multicast routing
   [RouterA-mrib] quit
   [RouterA] interface ethernet 1/1
   [RouterA-Ethernet1/1] igmp enable
   [RouterA-Ethernet1/1] pim sm
   [RouterA-Ethernet1/1] quit
   [RouterA] interface ethernet 1/2
   [RouterA-Ethernet1/2] pim sm
   [RouterA-Ethernet1/2] quit
   [RouterA] interface ethernet 1/3
   [RouterA-Ethernet1/3] pim sm
   [RouterA-Ethernet1/3] quit
   ```

   # Enable IP multicast routing, IGMP and PIM-SM on Router B and Router C in the same way Router A is configured. (Details not shown.)

   # Enable IP multicast routing and PIM-SM on Router D and Router E in the same way Router A is configured. (Details not shown.)
4. Configure C-BSRs and C-RPs:

   # On Router D, configure the service scope of RP advertisements, configure Ethernet 1/3 as a C-BSR and a C-RP, and set the hash mask length to 32 and the priority of the C-BSR to 10.

   ```
   <RouterD> system-view
   [RouterD] acl number 2005
   [RouterD-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
   [RouterD-acl-basic-2005] quit
   [RouterD] pim
   [RouterD-pim] c-bsr 192.168.4.2 hash-length 32 priority 10
   [RouterD-pim] c-rp 192.168.4.2 group-policy 2005
   [RouterD-pim] quit
   ```

   # On Router E, configure the service scope of RP advertisements, configure Ethernet 1/3 as a C-BSR and a C-RP, and set the hash mask length to 32 and the priority of the C-BSR to 20.

   ```
   <RouterE> system-view
   [RouterE] acl number 2005
   [RouterE-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
   [RouterE-acl-basic-2005] quit
   [RouterE] pim
   [RouterE-pim] c-bsr 192.168.9.2 hash-length 32 priority 20
   [RouterE-pim] c-rp 192.168.9.2 group-policy 2005
   [RouterE-pim] quit
   ```

Verifying the configuration

# Display PIM information on Router A.

```
[RouterA] display pim interface
 Interface           NbrCnt HelloInt   DR-Pri     DR-Address
 Eth1/1              0      30         1          10.110.1.1     (local)
 Eth1/2              1      30         1          192.168.1.2
 Eth1/3              1      30         1          192.168.9.2
```

# Display BSR information on Router A.

```
[RouterA] display pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:44
     Elected BSR address: 192.168.9.2
       Priority: 20
       Hash mask length: 32
       Uptime: 00:40:40
```

# Display BSR information on Router D.

```
[RouterD] display pim bsr-info
 Scope: non-scoped
     State: Candidate
     Bootstrap timer: 00:01:44
     Elected BSR address: 192.168.9.2
       Priority: 20
       Hash mask length: 32
       Uptime: 00:05:26
     Candidate BSR address: 192.168.4.2
       Priority: 10
       Hash mask length: 32
```

# Display BSR information on Router E.

```
[RouterE] display pim bsr-info
 Scope: non-scoped
     State: Elected
     Bootstrap timer: 00:01:44
     Elected BSR address: 192.168.9.2
       Priority: 20
       Hash mask length: 32
       Uptime: 00:01:18
     Candidate BSR address: 192.168.9.2
       Priority: 20
       Hash mask length: 32
```

# Display RP information on Router A.

```
[RouterA] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 225.1.1.0/24
       RP address              Priority  HoldTime  Uptime    Expires
       192.168.4.2             192       150       00:51:45  00:02:22
       192.168.9.2             192       150       00:51:45  00:02:22
```

PIM-SM admin-scoped zone configuration example

Network requirements

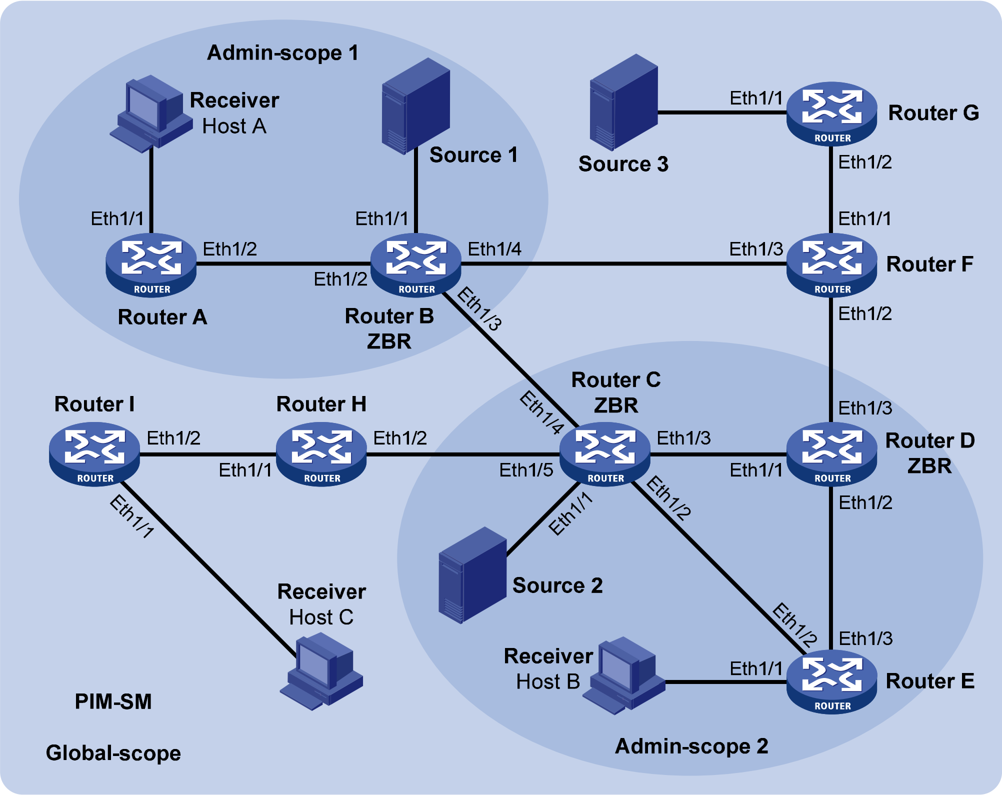
As shown in Figure 35, VOD streams are sent to receiver hosts in multicast. The entire PIM-SM domain is divided into admin-scoped zone 1, admin-scoped zone 2, and the global-scoped zone. Router B, Router C, and Router D are ZBRs of the three zones, respectively.

The source 1 and the source 2 send different multicast data to the multicast group 239.1.1.1. Host A receives the multicast data only from the source 1, and Host B receives the multicast data only from the source 2. The source 3 sends multicast data to the multicast group 224.1.1.1. Host C is a multicast receiver for the multicast group 224.1.1.1.

Ethernet 1/2 of Router B acts as a C-BSR and a C-RP for admin-scoped zone 1, and Ethernet 1/1 of Router D acts as a C-BSR and a C-RP for admin-scoped zone 2, and both of the two interfaces are designated to the multicast group range 239.0.0.0/8. Ethernet 1/1 of Router F acts as a C-BSR and a C-RP for the global-scoped zone, and is designated to all the multicast groups that are not in the range 239.0.0.0/8.

IGMPv2 runs between Router A, Router E, Router I, and the receivers that directly connect to them, respectively.

Figure 35 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Router A	Eth1/1	192.168.1.1/24	Router D	Eth1/1	10.110.5.2/24
	Eth1/2	10.110.1.1/24		Eth1/2	10.110.7.1/24
Router B	Eth1/1	192.168.2.1/24		Eth1/3	10.110.8.1/24
	Eth1/2	10.110.1.2/24	Router E	Eth1/1	192.168.4.1/24
	Eth1/3	10.110.2.1/24		Eth1/2	10.110.4.2/24

	Eth1/4	10.110.3.1/24		Eth1/3	10.110.7.2/24
Router C	Eth1/1	192.168.3.1/24	Router F	Eth1/1	10.110.9.1/24
	Eth1/2	10.110.4.1/24		Eth1/2	10.110.8.2/24
	Eth1/3	10.110.5.1/24		Eth1/3	10.110.3.2/24
	Eth1/4	10.110.2.2/24	Router G	Eth1/1	192.168.5.1/24
	Eth1/5	10.110.6.1/24		Eth1/2	10.110.9.2/24
Router H	Eth1/1	10.110.10.1/24	Source 1	-	192.168.2.10/24
	Eth1/2	10.110.6.2/24	Source 2	-	192.168.3.10/24
Router I	Eth1/1	192.168.6.1/24	Source 3	-	192.168.5.10/24
	Eth1/2	10.110.10.2/24			

Configuration procedure

1. Assign an IP address and subnet mask to each interface according to Figure 35. (Details not shown.)
2. Enable OSPF on all routers on the PIM-SM network to make sure the network-layer on the PIM-SM network is interoperable and the routing information among the routers can be dynamically updated. (Details not shown.)
3. Enable IP multicast routing, IGMP, and PIM-SM:

   # On Router A, enable IP multicast routing globally, enable IGMP on Ethernet 1/1, and enable PIM-SM on each interface.

   ```
   <RouterA> system-view
   [RouterA] multicast routing
   [RouterA-mrib] quit
   [RouterA] interface ethernet 1/1
   [RouterA-Ethernet1/1] igmp enable
   [RouterA-Ethernet1/1] pim sm
   [RouterA-Ethernet1/1] quit
   [RouterA] interface ethernet 1/2
   [RouterA-Ethernet1/2] pim sm
   [RouterA-Ethernet1/2] quit
   ```

   # Enable IP multicast routing, IGMP and PIM-SM on Router E and Router I in the same way Router A is configured. (Details not shown.)

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

   ```
   <RouterB> system-view
   [RouterB] multicast routing
   [RouterB-mrib] quit
   [RouterB] interface ethernet 1/1
   [RouterB-Ethernet1/1] pim sm
   [RouterB-Ethernet1/1] quit
   [RouterB] interface ethernet 1/2
   [RouterB-Ethernet1/2] pim sm
   [RouterB-Ethernet1/2] quit
   [RouterB] interface ethernet 1/3
   [RouterB-Ethernet1/3] pim sm
   [RouterB-Ethernet1/3] quit
   [RouterB] interface ethernet 1/4
   [RouterB-Ethernet1/4] pim sm
   ```

```
[RouterB-Ethernet1/4] quit
```

# Enable IP multicast routing and PIM-SM on Router C, Router D, Router F, Router G, and Router H in the same way Router B is configured. (Details not shown.)

4. Configure admin-scoped zone boundaries:

   # On Router B, configure Ethernet 1/3 and Ethernet 1/4 as the boundaries of admin-scoped zone 1.

   ```
   [RouterB] interface ethernet 1/3
   [RouterB-Ethernet1/3] multicast boundary 239.0.0.0 8
   [RouterB-Ethernet1/3] quit
   [RouterB] interface ethernet 1/4
   [RouterB-Ethernet1/4] multicast boundary 239.0.0.0 8
   [RouterB-Ethernet1/4] quit
   ```

   # On Router C, configure Ethernet 1/4 and Ethernet 1/5 as the boundaries of admin-scoped zone 2.

   ```
   <RouterC> system-view
   [RouterC] interface ethernet 1/4
   [RouterC-Ethernet1/4] multicast boundary 239.0.0.0 8
   [RouterC-Ethernet1/4] quit
   [RouterC] interface ethernet 1/5
   [RouterC-Ethernet1/5] multicast boundary 239.0.0.0 8
   [RouterC-Ethernet1/5] quit
   ```

   # On Router D, configure Ethernet 1/3 as the boundary of admin-scoped zone 2.

   ```
   <RouterD> system-view
   [RouterD] interface ethernet 1/3
   [RouterD-Ethernet1/3] multicast boundary 239.0.0.0 8
   [RouterD-Ethernet1/3] quit
   ```

5. Configure C-BSRs and C-RPs:

   # On Router B, configure the service scope of RP advertisements and configure Ethernet 1/2 as a C-BSR and a C-RP for admin-scoped zone 1.

   ```
   [RouterB] acl number 2001
   [RouterB-acl-basic-2001] rule permit source 239.0.0.0 0.255.255.255
   [RouterB-acl-basic-2001] quit
   [RouterB] pim
   [RouterB-pim] c-bsr 10.110.1.2 scope 239.0.0.0 8
   [RouterB-pim] c-rp 10.110.1.2 group-policy 2001
   [RouterB-pim] quit
   ```

   # On Router D, configure the service scope of RP advertisements and configure Ethernet 1/1 as a C-BSR and a C-RP for admin-scoped zone 2.

   ```
   [RouterD] acl number 2001
   [RouterD-acl-basic-2001] rule permit source 239.0.0.0 0.255.255.255
   [RouterD-acl-basic-2001] quit
   [RouterD] pim
   [RouterD-pim] c-bsr 10.110.5.2 scope 239.0.0.0 8
   [RouterD-pim] c-rp 10.110.5.2 group-policy 2001
   [RouterD-pim] quit
   ```

   # On Router F, configure Ethernet 1/1 as a C-BSR and a C-RP for the global-scoped zone.

   ```
   <RouterF> system-view
   ```

```
[RouterF] pim
[RouterF-pim] c-bsr 10.110.9.1
[RouterF-pim] c-rp 10.110.9.1
[RouterF-pim] quit
```

Verifying the configuration

# Display BSR information on Router B.

```
[RouterB] display pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:44
     Elected BSR address: 10.110.9.1
       Priority: 64
       Hash mask length: 30
       Uptime: 00:01:45

 Scope: 239.0.0.0/8
     State: Elected
     Bootstrap timer: 00:00:06
     Elected BSR address: 10.110.1.2
       Priority: 64
       Hash mask length: 30
       Uptime: 00:04:54
     Candidate BSR address: 10.110.1.2
       Priority: 64
       Hash mask length: 30
```

# Display BSR information on Router D.

```
[RouterD] display pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:44
     Elected BSR address: 10.110.9.1
       Priority: 64
       Hash mask length: 30
       Uptime: 00:01:45

 Scope: 239.0.0.0/8
     State: Elected
     Bootstrap timer: 00:01:12
     Elected BSR address: 10.110.5.2
       Priority: 64
       Hash mask length: 30
       Uptime: 00:03:48
     Candidate BSR address: 10.110.5.2
       Priority: 64
       Hash mask length: 30
```

# Display BSR information on Router F.

```
[RouterF] display pim bsr-info
```

```
 Scope: non-scoped
     State: Elected
     Bootstrap timer: 00:00:49
     Elected BSR address: 10.110.9.1
       Priority: 64
       Hash mask length: 30
       Uptime: 00:11:11
     Candidate BSR address: 10.110.9.1
       Priority: 64
       Hash mask length: 30
```

# Display RP information on Router B.

```
[RouterB] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       RP address               Priority  HoldTime  Uptime    Expires
       10.110.9.1               192       150       00:03:39  00:01:51
   Scope: 239.0.0.0/8
     Group/MaskLen: 239.0.0.0/8
       RP address               Priority  HoldTime  Uptime    Expires
       10.110.1.2 (local)       192       150       00:07:44  00:01:51
```

# Display RP information on Router D.

```
[RouterD] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       RP address               Priority  HoldTime  Uptime    Expires
       10.110.9.1               192       150       00:03:42  00:01:48
   Scope: 239.0.0.0/8
     Group/MaskLen: 239.0.0.0/8
       RP address               Priority  HoldTime  Uptime    Expires
       10.110.5.2 (local)       192       150       00:06:54  00:02:41
```

# Display RP information on Router F.

```
[RouterF] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: 224.0.0.0/4
       RP address               Priority  HoldTime  Uptime    Expires
       10.110.9.1 (local)       192       150       00:00:32  00:01:58
```

PIM-SSM configuration example

Network requirements

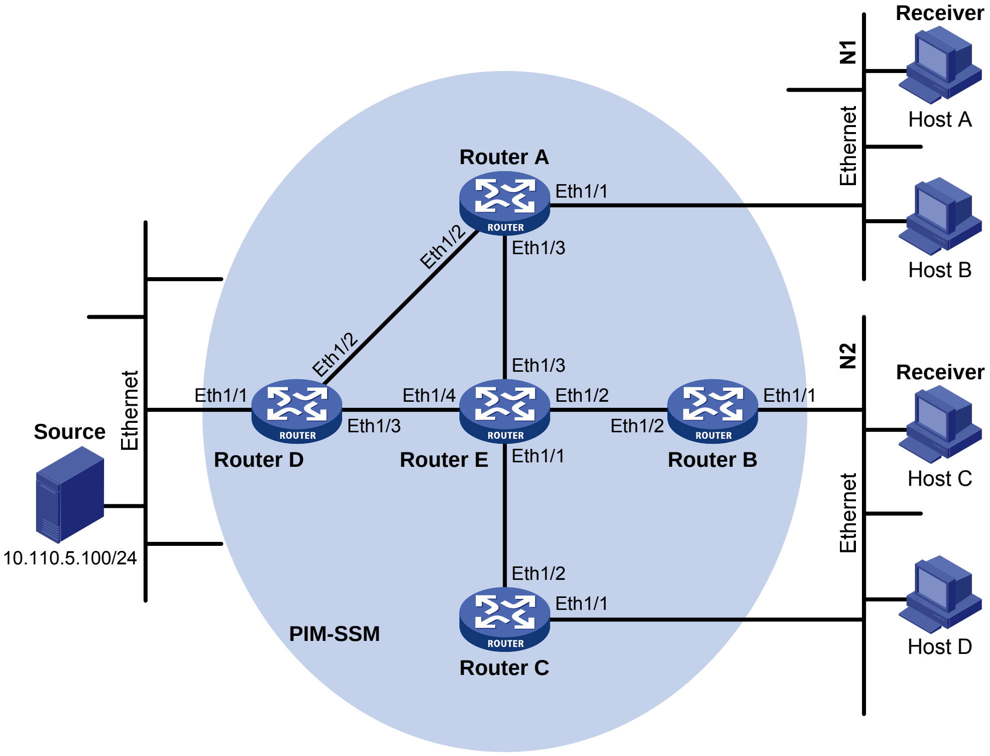
As shown in Figure 36, the receivers receive VOD information through multicast. The receiver groups of different organizations form stub networks, and one or more receiver hosts exist in each stub network. The entire PIM domain operates in the SSM mode.

Host A and Host C are multicast receivers in two stub networks.

The SSM group range is 232.1.1.0/24.

IGMPv3 runs between Router A and N1 and between Router B, Router C, and N2.

Figure 36 Network diagram



Device	Interface	IP address	Device	Interface	IP address
Router A	Eth1/1	10.110.1.1/24	Router D	Eth1/1	10.110.5.1/24
	Eth1/2	192.168.1.1/24		Eth1/2	192.168.1.2/24
	Eth1/3	192.168.9.1/24		Eth1/3	192.168.4.2/24
Router B	Eth1/1	10.110.2.1/24	Router E	Eth1/1	192.168.3.2/24
	Eth1/2	192.168.2.1/24		Eth1/2	192.168.2.2/24
Router C	Eth1/1	10.110.2.2/24		Eth1/3	192.168.9.2/24
	Eth1/2	192.168.3.1/24		Eth1/4	192.168.4.1/24

Configuration procedure

1. Assign an IP address and subnet mask to each interface according to Figure 36. (Details not shown.)
2. Configure OSPF on the routers in the PIM-SSM domain to make sure they are interoperable at the network layer. (Details not shown.)
3. Enable IP multicast routing, IGMP and PIM-SM:

   # On Router A, enable IP multicast routing globally, enable IGMPv3 on Ethernet 1/1, and enable PIM-SM on each interface.

   ```
   <RouterA> system-view
   [RouterA] multicast routing
   [RouterA-mrib] quit
   [RouterA] interface ethernet 1/1
   ```

```
[RouterA-Ethernet1/1] igmp enable
[RouterA-Ethernet1/1] igmp version 3
[RouterA-Ethernet1/1] pim sm
[RouterA-Ethernet1/1] quit
[RouterA] interface ethernet 1/2
[RouterA-Ethernet1/2] pim sm
[RouterA-Ethernet1/2] quit
[RouterA] interface ethernet 1/3
[RouterA-Ethernet1/3] pim sm
[RouterA-Ethernet1/3] quit
```

# Enable IP multicast routing, IGMP, and PIM-SM on Router B and Router C in the same way Router A is configured. (Details not shown.)

# Enable IP multicast routing and PIM-SM on Router D and Router E in the same way Router A is configured. (Details not shown.)

4. Configure the SSM group range:

# Configure the SSM group range to be 232.1.1.0/24 on Router A.

```
[RouterA] acl number 2000
[RouterA-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[RouterA-acl-basic-2000] quit
[RouterA] pim
[RouterA-pim] ssm-policy 2000
[RouterA-pim] quit
```

# Configure the SSM group range on Router B, Router C, Router D and Router E in the same way Router A is configured. (Details not shown.)

Verifying the configuration

Use the **display pim interface** command to display the PIM information on each interface. For example:

# Display PIM configuration information on Router A.

```
[RouterA] display pim interface
 Interface            NbrCnt HelloInt   DR-Pri     DR-Address
 Eth1/1               0      30         1          10.110.1.1     (local)
 Eth1/2               1      30         1          192.168.1.2
 Eth1/3               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). Router A builds an SPT toward the multicast source. Routers on the SPT path (Router A and Router D) have generated (S, G) entry, but Router E, which is not on the SPT path, does not have multicast routing entries. You can use the **display pim routing-table** command to display the PIM routing table information on each router. For example:

# Display PIM routing table information on Router A.

```
[RouterA] display pim routing-table
 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: Ethernet1/2
         Upstream neighbor: 192.168.1.2
         RPF prime neighbor: 192.168.1.2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Ethernet1/1
             Protocol: igmp, UpTime: 00:13:25, Expires: 00:03:25
```

# Display PIM routing table information on Router D.

```
[RouterD] display pim routing-table
 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: Ethernet1/1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Ethernet1/2
             Protocol:  pim-ssm, UpTime: 00:12:05, Expires: 00:03:25
```

Troubleshooting PIM

A multicast distribution tree cannot be correctly built

Symptom

A multicast distribution tree cannot be correctly built because no multicast forwarding entries are established on the routers (including routers directly connected with multicast sources or receivers) in a PIM network.

Analysis

- On a PIM-DM enabled network, multicast data is flooded from the router that directly connects to the multicast source to the routers that directly connects to the receivers. When the multicast data is flooded to a router, the router creates an (S, G) entry 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 RPF interface toward the multicast source, the router cannot create an (S, G) entry.
- On a PIM-SM enabled network, when a router wants to join the SPT, the router creates an (S, G) entry 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-SM is not enabled on the RPF interface toward the multicast source, the router cannot create an (S, G) entries.
- When a multicast router receives a multicast packet, it looks up the existing unicast routing table for the optimal route to the packet source. The outgoing interface of this route act as the RPF interface and the next hop acts the RPF neighbor. The RPF interface completely relies on the existing unicast route and is independent of PIM. The RPF interface must be enabled with PIM, and the RPF neighbor must be a PIM neighbor. If PIM is not enabled on the RPF interface or the RPF neighbor, the multicast distribution tree cannot be built correctly, causing abnormal multicast forwarding.
- Because a hello message does not carry PIM mode information, a PIM router cannot identify what PIM mode its PIM neighbor is running. If the RPF interface on a router and the connected interface

of the router's RPF neighbor operate in different PIM modes, the multicast distribution tree cannot be built correctly, causing abnormal multicast forwarding.

- The same PIM mode must run on the entire network. Otherwise, the multicast distribution tree cannot be built correctly, causing abnormal multicast forwarding.

Solution

1. Use **display ip routing-table** to verify that a unicast route to the multicast source or the RP is available.
2. Use **display pim interface** to verify PIM information on each interface, especially on the RPF interface. If PIM is not enabled on the interfaces, use **pim dm** or **pim sm** to enable PIM-DM or PIM-SM for the interfaces.
3. Use **display pim neighbor** to verify that the RPF neighbor is a PIM neighbor.
4. Verify that PIM and IGMP are enabled on the interfaces that directly connect to the multicast sources or the receivers.
5. Use **display pim interface verbose** to verify that the same PIM mode is enabled on the RPF interface on a router and the connected interface of the router's RPF neighbor.
6. Use **display current-configuration** to verify that the same PIM mode is enabled on all routers. For PIM-SM, verify that the BSR and C-RPs are correctly configured.

Multicast data is 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 multicast data but does not create an (S, G) entry in the PIM routing table.

Analysis

- If a multicast forwarding boundary has been configured through the **multicast boundary** command, and the multicast packets are kept from crossing the boundary, PIM cannot create routing entries for the packets.
- If an ACL is defined by the **source-policy** command, and the multicast packets cannot match the ACL rule, PIM cannot create the routing entries for the packets.

Solution

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

An RP cannot join an SPT in PIM-SM

Symptom

An RPT cannot be correctly built, or an RP cannot join the SPT toward the multicast source.

Analysis

- RPs are the core of a PIM-SM domain. An RP provides services for a specific multicast group, and multiple RPs can coexist on a network. Make sure the RP information on all routers is exactly the same to map a specific multicast group to the same RP. Otherwise, multicast forwarding fails.
- If a static RP is configured, use the same static RP configuration on all routers on the entire network. Otherwise, multicast forwarding fails.

Solution

1. Use **display ip routing-table** to verify that a unicast route to the RP is available on each router.
2. Use **display pim rp-info** to verify that the dynamic RP information is consistent on all routers.
3. Use **display pim rp-info** to verify that the same static RPs are configured on all routers on the network.

An RPT cannot be built or multicast source registration fails in PIM-SM

Symptom

The C-RPs cannot unicast advertisement messages to the BSR. The BSR does not advertise BSMs containing C-RP information and has no unicast route to any C-RP. An RPT cannot be correctly established, or the source-side DR cannot register the multicast source with the RP.

Analysis

- The C-RPs periodically send advertisement messages to the BSR by unicast. If a C-RP has no unicast route to the BSR, it cannot send advertisement messages to the BSR, and the BSR cannot advertise BSMs containing the information of the C-RP.
- If the BSR does not have a unicast route to a C-RP, it discards the advertisement messages from the C-RP. Therefore, the BSR cannot advertise BSMs containing the information of the C-RP.
- RPs are the core of a PIM-SM domain. Make sure the RP information on all routers is exactly the same to map a specific multicast group to the same RP, and a unicast route to the RP is available on the routers.

Solution

1. Use **display ip routing-table** to verify that unicast routes to the C-RPs and the BSR are available on each router and that a route is available between each C-RP and the BSR. Make sure each C-RP has a unicast route to the BSR, the BSR has a unicast route to each C-RP, and each router on the network has unicast routes to the C-RPs.
2. Use **display pim bsr-info** to verify that the BSR information exists on each router, and then use **display pim rp-info** to verify that the RP information is correct on each router.
3. Use **display pim neighbor** to verify that PIM neighboring relationship has been correctly established among the routers.

Configuring IPv6 multicast routing and forwarding

Overview

IPv6 multicast routing and forwarding uses the following tables:

- IPv6 multicast protocols' routing tables, such as the IPv6 PIM routing table.
- General IPv6 multicast routing table that summarizes the multicast routing information generated by different IPv6 multicast routing protocols. The IPv6 multicast routing information from IPv6 multicast sources to IPv6 multicast groups are stored in a set of (S, G) routing entries.
- IPv6 multicast forwarding table that guides IPv6 multicast forwarding. The optimal routing entries in the IPv6 multicast routing table are added to the IPv6 multicast forwarding table.

RPF check mechanism

An IPv6 multicast routing protocol relies on the existing IPv6 unicast routing information in creating IPv6 multicast routing entries. When creating IPv6 multicast routing table entries, an IPv6 multicast routing protocol uses the reverse path forwarding (RPF) check mechanism to ensure IPv6 multicast data delivery along the correct path. The RPF check mechanism also helps avoid data loops.

A multicast routing protocol uses the IPv6 unicast routing table to perform the RPF check. The IPv6 unicast routing table contains unicast routing information.

RPF check process

When performing an RPF check, the router searches its IPv6 unicast routing table by using the IPv6 address of the packet source as the destination address and automatically selects an optimal route. The outgoing interface of the route is the RPF interface and the next hop is the RPF neighbor. The router considers the path of the IPv6 multicast packet that the RPF interface receives from the RPF neighbor as the shortest path that leads back to the source.

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

- For a packet that travels along the SPT from the multicast source to the receivers or the RP, the packet source for RPF check is the multicast source.
- For a packet that travels along the RPT from the RP to the receivers, or along the source-side RPT from the multicast source to the RP, the packet source for RPF check is the RP.
- For a bootstrap message from the BSR, the packet source for RPF check is the BSR.

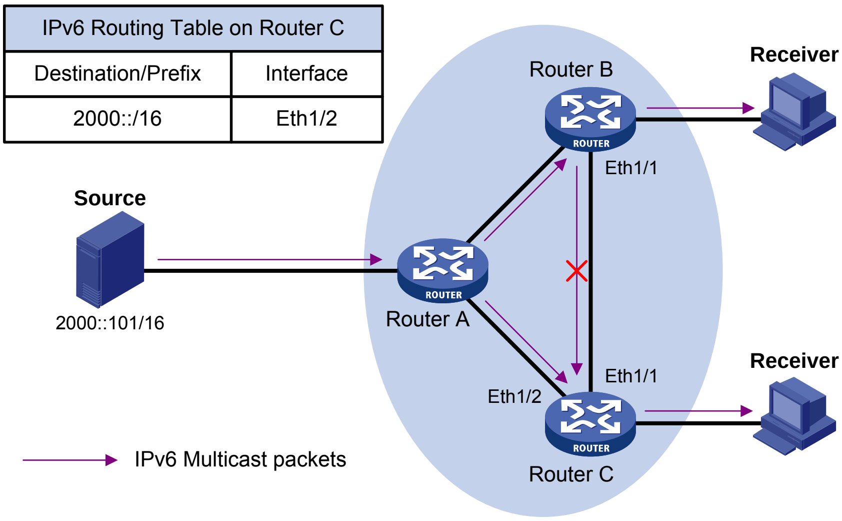
For more information about the concepts of SPT, RPT, source-side RPT, RP, and BSR, see "Configuring IPv6 PIM."

RPF check implementation in IPv6 multicast

Implementing an RPF check on each received IPv6 multicast packet would heavily burden the router. The use of an IPv6 multicast forwarding table is the solution to this issue. When the router creates an IPv6 multicast routing entry and an IPv6 multicast forwarding entry for an IPv6 multicast packet, it sets the RPF interface of the packet as the incoming interface of the forwarding entry. After the router receives an IPv6 multicast packet, it searches its IPv6 multicast forwarding table:

- If no forwarding entry matches the packet, the packet undergoes an RPF check. The router creates an IPv6 multicast routing entry with the RPF interface as the incoming interface and installs the entry into the IPv6 multicast forwarding table.
  - If the interface that received the packet is the RPF interface, the RPF check succeeds and the router forwards the packet out of all outgoing interfaces.
  - If the interface that received the packet is not the RPF interface, the RPF check fails and the router discards the packet.
- If a forwarding entry matches the packet, and the interface that received the packet is the incoming interface of the forwarding entry, the router forwards the packet out of all outgoing interfaces.
- If a forwarding entry matches the packet, but the interface that received the packet is not the incoming interface of the forwarding entry, the IPv6 multicast packet undergoes an RPF check.
  - If the RPF interface is the incoming interface, it indicates that the forwarding entry is correct but the packet traveled along a wrong path. The router discards the packet.
  - If the RPF interface is not the incoming interface, it indicates that the forwarding entry has expired, and the router replaces the incoming interface with the RPF interface. If the interface that received the packet is the RPF interface, the router forwards the packet out of all outgoing interfaces. Otherwise, it discards the packet.

Figure 37 RPF check process



IPv6 Routing Table on Router C	
Destination/Prefix	Interface
2000::/16	Eth1/2

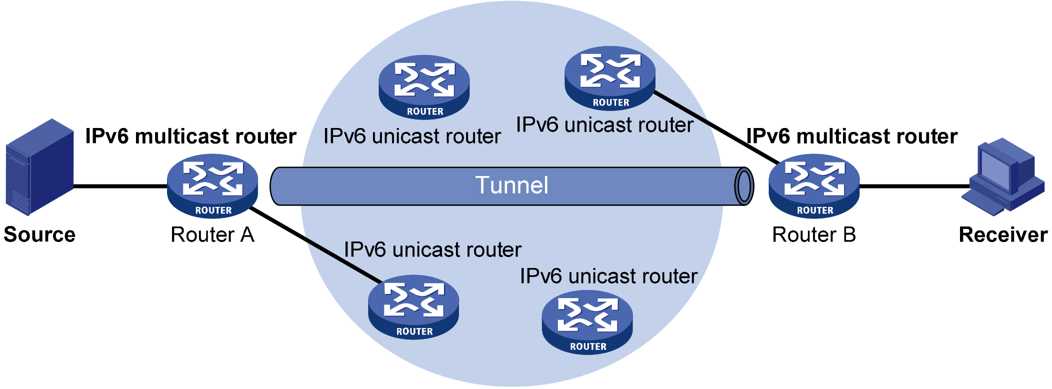
As shown in Figure 37, assume that IPv6 unicast routes are available in the network, and IPv6 multicast packets travel along the SPT from the multicast source to the receivers. The IPv6 multicast forwarding table on Router C contains the (S, G) entry, with Ethernet 1/2 as the RPF interface.

- When Ethernet 1/2 of Router C receives an IPv6 multicast packet, because the interface is the incoming interface of the (S, G) entry, the router forwards the packet out of all outgoing interfaces.
- When Ethernet 1/1 of Router C receives an IPv6 multicast packet, because the interface is not the incoming interface of the (S, G) entry, the router performs an RPF check on the packet. The router searches its IPv6 unicast routing table and finds that the outgoing interface to the source (the RPF interface) is Ethernet 1/2. This means that the (S, G) entry is correct but the packet traveled along a wrong path. The RPF check fails and the router discards the packet.

IPv6 multicast forwarding across IPv6 unicast subnets

Routers forward the IPv6 multicast data from an IPv6 multicast source hop by hop along the forwarding tree, but some routers might not support IPv6 multicast protocols in a network. When the IPv6 multicast data is forwarded to a router that does not support IPv6 multicast, the forwarding path is blocked. In this case, you can enable IPv6 multicast data forwarding across the IPv6 unicast subnets by establishing a tunnel between the routers at both ends of the IPv6 unicast subnets.

Figure 38 IPv6 multicast data transmission through a tunnel



As shown in Figure 38, with a tunnel established between the multicast routers Router A and Router B, Router A encapsulates the IPv6 multicast data in unicast IPv6 packets, and forwards them to Router B across the tunnel through unicast routers. Then, Router B strips off the unicast IPv6 header and continues to forward the IPv6 multicast data down toward the receivers.

Configuration task list

Tasks at a glance
(Required.) Enabling IPv6 multicast routing
(Optional.) Configuring IPv6 multicast routing and forwarding • (Optional.) Configuring the RPF route selection rule • (Optional.) Configuring IPv6 multicast load splitting • (Optional.) Configuring an IPv6 multicast forwarding boundary • (Optional.) Configuring IPv6 static multicast MAC address entries

Enabling IPv6 multicast routing

Enable IPv6 multicast routing before you configure any Layer 3 IPv6 multicast functionality in the public network or VPN instance.

To enable IPv6 multicast routing:

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

Step		Command	Remarks
2.	Enable IPv6 multicast routing and enter IPv6 MRIB view.	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	By default, IPv6 multicast routing is disabled.

Configuring IPv6 multicast routing and forwarding

Before you configure IPv6 multicast routing and forwarding, complete the following tasks:

- 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.

Configuring the RPF route selection rule

You can configure the router to select the RPF route based on the longest prefix match principle. For more information about RPF route selection, see "RPF check process."

To configure an IPv6 multicast routing policy:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter IPv6 MRIB view.	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure the device to select the RPF route based on the longest prefix match.	**longest-match**	By default, the route with the highest priority is selected as the RPF route.

Configuring IPv6 multicast load splitting

By configuring per-source or per-source-and-group load splitting, you can optimize the traffic delivery when multiple IPv6 multicast data streams are handled.

To configure IPv6 multicast load splitting:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter IPv6 MRIB view.	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure IPv6 multicast load splitting.	**load-splitting** {**source** | **source-group** }	By default, IPv6 multicast load splitting is disabled.

Configuring an IPv6 multicast forwarding boundary

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. 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 is not forwarded. Once an IPv6 multicast boundary is configured on an interface, this interface can no longer forward IPv6 multicast packets (including those sent from the local device) or receive IPv6 multicast packets.

TIP:

You do not need to enable IPv6 multicast routing before this configuration.

To configure an IPv6 multicast forwarding boundary:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Configure an IPv6 multicast forwarding boundary.	**ipv6 multicast boundary** { *ipv6-group-address prefix-length* | **scope** { *scope-id* | **admin-local** | **global** | **organization-local** | **site-local** } }	By default, no forwarding boundary is configured.

Configuring IPv6 static multicast MAC address entries

This feature is available only on the MSR series routers with Ethernet Layer 2 switching interface modules. For information about the Ethernet Layer 2 switching interface modules, see *HP MSR Router Series Interface Module Guide*.

In Layer-2 multicast, a Layer-2 IPv6 multicast protocol (such as MLD snooping) can dynamically add IPv6 multicast MAC address entries. Or, you can manually configure IPv6 multicast MAC address entries.

TIP:

- You do not need to enable IPv6 multicast routing before this configuration.
- The IPv6 multicast MAC address that can be configured in the MAC address entry must be unused. (The least significant bit of the most significant octet is 1.)

You can configure IPv6 static multicast MAC address entries on the specified interface in system view, or on the current interface in interface view.

To configure an IPv6 static multicast MAC address entry in system view:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a static multicast MAC address entry.	**mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	By default, no static multicast MAC address entries exist.

To configure an IPv6 static multicast MAC address entry in interface view:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure a static multicast MAC address entry.	**mac-address multicast** *mac-address* **vlan** *vlan-id*	By default, no static multicast MAC address entries exist.

Displaying and maintaining IPv6 multicast routing and forwarding

△ CAUTION:

The **reset** commands might cause IPv6 multicast data transmission failures.

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display information about IPv6 static multicast MAC address table.	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]]
Display information about the interfaces maintained by the IPv6 MRIB.	**display ipv6 mrib** [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*]
Display IPv6 multicast boundary information.	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **boundary** { **group** [*ipv6-group-address* [*prefix-length*]] | **scope** [*scope-id*] } [**interface** *interface-type interface-number*]
Display statistics for IPv6 multicast forwarding events (MSR2000/MSR3000).	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding event**
Display statistics for IPv6 multicast forwarding events (MSR4000).	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding event** [**slot** *slot-number*]
Display information about the IPv6 multicast forwarding table (MSR2000/MSR3000).	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number* | **statistics**] *
Display information about the IPv6 multicast forwarding table (MSR4000).	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number* | **slot** *slot-number* | **statistics**] *
Display information about the IPv6 multicast routing table.	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **routing-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** *interface-type interface-number* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *

Task	Command
Display the RPF route information of the specified IPv6 multicast source.	**display ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **rpf-info** *ipv6-source-address* [*ipv6-group-address*]
Clear statistics for IPv6 multicast forwarding events.	**reset ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding event**
Clear forwarding entries from the IPv6 multicast forwarding table.	**reset ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **forwarding-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* } } * | **all** }
Clear routing entries from the IPv6 multicast routing table.	**reset ipv6 multicast** [**vpn-instance** *vpn-instance-name*] **routing-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** *interface-type interface-number* } * | **all** }

NOTE:

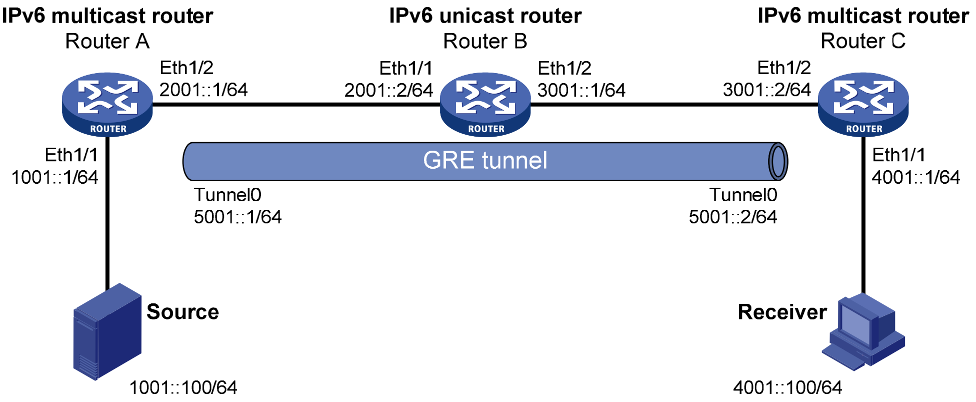
When a routing entry is removed, the associated forwarding entry is also removed. When a forwarding entry is removed, the associated routing entry is also removed.

Multicast forwarding over a GRE tunnel

Network requirements

As shown in Figure 39, IPv6 multicast routing and IPv6 PIM-DM are enabled on Router A and Router C. Router B does not support IPv6 multicast. OSPFv3 is running on Router A, Router B, and Router C. Configure a GRE tunnel so that the receiver host can receive the IPv6 multicast data from the source.

Figure 39 Network diagram



Configuration procedure

1. Configure the IP address and prefix length for each interface as shown in Figure 39. (Details not shown.)
2. Enable OSPFv3 on the routers to make sure the network-layer among the routers is interoperable and the routing information among the routers can be dynamically updated. (Details not shown.)

3. Configure a GRE tunnel:

   # Create interface Tunnel 0 on Router A and specify the tunnel encapsulation mode as GRE over IPv6.

```
<RouterA> system-view
[RouterA] interface tunnel 0 mode gre ipv6
```

   # Configure the IPv6 address for interface Tunnel 0 on Router A and specify its source and destination addresses.

```
[RouterA-Tunnel0] ipv6 address 5001::1 64
[RouterA-Tunnel0] source 2001::1
[RouterA-Tunnel0] destination 3001::2
[RouterA-Tunnel0] quit
```

   # Create interface Tunnel 0 on Router C and specify the tunnel encapsulation mode as GRE over IPv6.

```
<RouterC> system-view
[RouterC] interface tunnel 0 mode gre ipv6
```

   # Configure the IPv6 address for interface Tunnel 0 and specify its source and destination addresses.

```
[RouterC-Tunnel0] ipv6 address 5001::2 64
[RouterC-Tunnel0] source 3001::2
[RouterC-Tunnel0] destination 2001::1
[RouterC-Tunnel0] quit
```

4. Enable IPv6 multicast routing, IPv6 PIM-DM, and MLD:

   # On Router A, enable IPv6 multicast routing, and enable IPv6 PIM-DM on each interface.

```
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] ipv6 pim dm
[RouterA-Ethernet1/1] quit
[RouterA] interface ethernet 1/2
[RouterA-Ethernet1/2] ipv6 pim dm
[RouterA-Ethernet1/2] quit
[RouterA] interface tunnel 0
[RouterA-Tunnel0] ipv6 pim dm
[RouterA-Tunnel0] quit
```

   # On Router C, enable IPv6 multicast routing, enable MLD on Ethernet 1/1, and enable IPv6 PIM-DM on each interface.

```
[RouterC] ipv6 multicast routing
[RouterC-mrib6] quit
[RouterC] interface ethernet 1/1
[RouterC-Ethernet1/1] mld enable
[RouterC-Ethernet1/1] ipv6 pim dm
[RouterC-Ethernet1/1] quit
[RouterC] interface ethernet 1/2
[RouterC-Ethernet1/2] ipv6 pim dm
[RouterC-Ethernet1/2] quit
[RouterC] interface tunnel 0
[RouterC-Tunnel0] ipv6 pim dm
```

```
[RouterC-Tunnel0] quit
```

Verifying the configuration

The source sends the IPv6 multicast data to the IPv6 multicast group FF1E::101 and the receiver host can receive the IPv6 multicast data after joining the IPv6 multicast group. You can use the **display ipv6 pim routing-table** command to display IPv6 PIM routing table information on routers. For example:

# Display PIM routing table information on Router C.

```
[RouterC] display ipv6 pim routing-table
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, FF1E::101)
     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: Ethernet1/1
             Protocol: mld, UpTime: 00:04:25, Expires: never

 (1001::100, FF1E::101)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:06:14
     Upstream interface: Tunnel0
         Upstream neighbor: FE80::A01:101:1
         RPF prime neighbor: FE80::A01:101:1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Ethernet1/1
             Protocol: pim-dm, UpTime: 00:04:25, Expires: never
```

The output shows that Router A is the RPF neighbor of Router C and the IPv6 multicast data from Router A is delivered over a GRE tunnel to Router C.

Configuring MLD

Overview

Multicast Listener Discovery (MLD) establishes and maintains IPv6 multicast group memberships between a Layer 3 multicast device and its directly connected hosts.

MLD has two versions:

- MLDv1 (defined by RFC 2710), which is derived from IGMPv2.
- MLDv2 (defined by RFC 3810), which is derived from IGMPv3.

The two MLD versions support the ASM model. In addition, MLDv2 can directly implement the SSM model, but MLDv1 must work with the MLD SSM mapping function to implement the SSM model. For more information about the ASM and SSM models, see "Multicast overview."

How MLDv1 works

MLDv1 implements IPv6 multicast listener management based on the query and response mechanism.

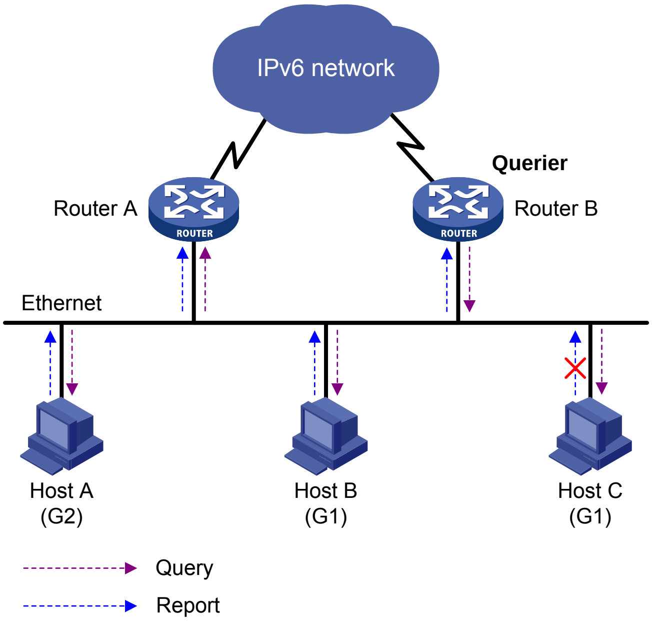
Electing the MLD querier

All IPv6 multicast routers that run MLD on the same subnet can monitor MLD listener report messages (often called "reports") from hosts, but the subnet needs only one router to act as the MLD querier to send MLD query messages (often called "queries"). A querier election mechanism determines which router acts as the MLD querier on the subnet.

1. Initially, every MLD router assumes itself as the querier and sends MLD general query messages (often called "general queries") to all hosts and routers on the local subnet. The destination address of the messages is FF02::1.
2. After receiving a general query, every MLD router compares the source IPv6 address of the query with its own link-local interface address. After comparison, the router with the lowest IPv6 address wins the querier election and all other routers become non-queriers.
3. All the non-queriers start a timer called the "other querier present timer." If a router receives an MLD query from the querier before the timer expires, it resets this timer. Otherwise, it assumes the querier has timed out and initiates a new querier election process.

Joining an IPv6 multicast group

Figure 40 MLD queries and reports



As shown in Figure 40, assume that Host B and Host C want to receive the IPv6 multicast data addressed to IPv6 multicast group G1, and Host A wants to receive the IPv6 multicast data addressed to G2. The following process describes how the hosts join the IPv6 multicast groups and how the MLD querier (Router B in Figure 40) maintains the IPv6 multicast group memberships:

1. The hosts send unsolicited MLD reports to the IPv6 multicast groups they want to 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 FF02::1) to all hosts and routers on the local subnet.
3. After receiving a query, Host B or Host C (the delay timer of whichever expires first) sends an MLD report to the IPv6 multicast group G1 to announce its membership for G1. Assume that Host B sends the report. After hearing the report from Host B, Host C, which is on the same subnet as Host B, suppresses its own report for G1 because the MLD routers (Router A and Router B) already know that at least one host on the local subnet is interested in G1. This mechanism, known as the "MLD report suppression," helps reduce traffic on the local subnet.
4. At the same time, because Host A is interested in G2, it sends a report to the IPv6 multicast group G2.
5. Through the query/report process, the MLD routers learn that G1 and G2 have members on the local subnet, and the IPv6 multicast routing protocol (for example, IPv6 PIM) that is running on the routers generates (*, G1) and (*, G2) multicast forwarding entries. These entries are the basis for subsequent IPv6 multicast forwarding. The asterisk (*) represents any IPv6 multicast source.
6. When the IPv6 multicast data addressed to G1 or G2 reaches an MLD router, the router forwards the IPv6 multicast data to the local subnet according to the (*, G1) and (*, G2) multicast forwarding entries, 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. After receiving the MLD done message, the querier sends a configurable number of multicast-address-specific queries to the group that the host is leaving. The IPv6 multicast addresses queried include both the destination address field and the group address field of the message.
3. One of the remaining members (if any on the subnet) of the group sends a report within the time of the maximum response delay advertised in the query messages.
4. If the querier receives a report for the group within the maximum response delay time, it maintains the memberships of the IPv6 multicast group. Otherwise, the querier assumes that no hosts on the subnet are interested in IPv6 multicast traffic addressed to that group and stops maintaining the memberships of the group.

MLDv2 enhancements

MLDv2 is based on and backwards-compatible with MLDv1. MLDv2 provides hosts with enhanced control capabilities and enhances the MLD state.

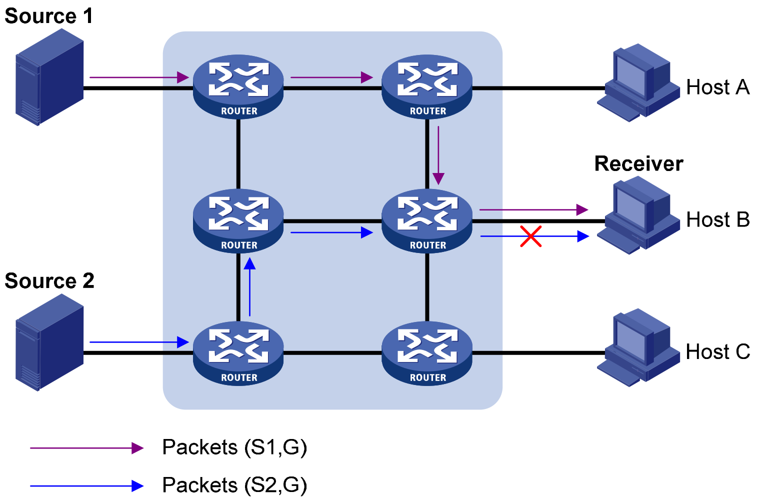
Enhancements in control capability of hosts

MLDv2 has introduced IPv6 multicast source filtering modes (Include and Exclude). These modes allow a host to join a designated IPv6 multicast group and to choose whether to receive or reject multicast data from designated IPv6 multicast sources. When a host joins an IPv6 multicast group, one of the following occurs:

- If the host 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 the host 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 41, the network comprises two IPv6 multicast sources, Source 1 (S1) and Source 2 (S2), both of which can send IPv6 multicast data to IPv6 multicast group G. Host B is interested only in the IPv6 multicast data that Source 1 sends to G but not in the data from Source 2.

Figure 41 Flow paths of multicast-address-and-source-specific multicast traffic



In MLDv1, Host B cannot select IPv6 multicast sources when it joins IPv6 multicast group G, and IPv6 multicast streams from both Source 1 and Source 2 flow to Host B whether it needs them or not.

When MLDv2 runs on the hosts and routers, Host B can explicitly express its interest in the IPv6 multicast data that Source 1 sends to G (denoted as (S1, G)), rather than the IPv6 multicast data that Source 2 sends to G (denoted as (S2, G)). Only IPv6 multicast data from Source 1 is delivered to Host B.

Enhancement in MLD state

A multicast router that is running MLDv2 maintains the multicast address state for each multicast address on each attached subnet. The multicast address state consists of the following information:

- **Filter mode**—Router keeps tracing the Include or Exclude state.
- **List of sources**—Router keeps tracing the newly added or deleted IPv6 multicast source.
- **Timers**—Filter timers which includes the time that the router waits before switching to the Include mode after an IPv6 multicast address times out, and the source timers for source recording.

MLD support for VPNs

MLD maintains group memberships on a per-interface base. After receiving an MLD message on an interface, MLD processes the packet within the VPN to which the interface belongs. MLD only communicates with other multicast protocols within the same VPN instance.

Protocols and standards

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

MLD configuration task list

Task at a glance
Configuring basic MLD functions • (Required.) Enabling MLD • (Optional.) Specifying the MLD version • (Optional.) Configuring an interface as a static member interface • (Optional.) Configuring an IPv6 multicast group filter
Adjusting MLD performance (Optional.) Enabling MLD fast-leave processing

Configuring basic MLD functions

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

- Enable IPv6 forwarding and configure an IPv6 unicast routing protocol so that all devices can be interoperable at the network layer.
- Configure IPv6 PIM.
- 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.

Enabling MLD

Enable MLD on the interface on which IPv6 multicast group memberships are created and maintained.

To enable MLD:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable IPv6 multicast routing and enter IPv6 MRIB view.	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	Disable by default.
3.	Return to system view.	**quit**	N/A
4.	Enter interface view.	**interface** *interface-type interface-number*	N/A
5.	Enable MLD.	**mld enable**	Disabled by default.

Specifying the MLD version

Because MLD message types and formats vary with MLD versions, configure the same MLD version for all routers on the same subnet. Otherwise, MLD cannot operate correctly.

To specify an MLD version:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure an MLD version on the interface.	**mld version** *version-number*	MLDv1 by default.

Configuring an interface as a static member interface

You can configure an interface as a static member of an IPv6 multicast group or an IPv6 multicast source and group, so that the interface can receive IPv6 multicast data addressed to that IPv6 multicast group for the purpose of testing IPv6 multicast data forwarding.

Configuration guidelines

- A static member interface has the following restrictions:
  - If the interface is MLD and IPv6 PIM-SM enabled, it must be an IPv6 PIM-SM DR.
  - If the interface is MLD enabled but not IPv6 PIM-SM enabled, it must be an MLD querier.

  For more information about IPv6 PIM-SM and DR, see "Configuring IPv6 PIM."
- A static member interface does not respond to queries from the MLD querier. When you configure an interface as a static member interface or cancel this configuration on the interface, the interface

does not send any MLD report or an MLD done message without a request. This is because the interface is not a real member of the IPv6 multicast group or the IPv6 multicast source and group.

Configuration procedure

To configure an interface as a static member interface:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure the interface as a static member interface.	**mld static-group** *ipv6-group-address* [**source** *ipv6-source-address*]	By default, an interface is not a static member of any IPv6 multicast group or IPv6 multicast source and group.

Configuring an IPv6 multicast group filter

To restrict the hosts on the network attached to an interface from joining certain IPv6 multicast groups, you can specify an IPv6 ACL on the interface as a packet filter so that the interface maintains only the IPv6 multicast groups that match the criteria.

To configure an IPv6 multicast group filter:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure an IPv6 multicast group filter.	**mld group-policy** *acl6-number* [*version-number*]	By default, no IPv6 group filter is configured on the interface. The hosts on the current interface can join any multicast group.

NOTE:

If you configure the interface as a static member interface for an IPv6 multicast group or an IPv6 multicast source and group, this configuration does not take effect on the IPv6 multicast group or the IPv6 multicast source and group.

Adjusting MLD performance

Before adjusting MLD performance, complete the following tasks:

- Enable IPv6 forwarding and configure an IPv6 unicast routing protocol so that all devices can be interoperable at the network layer.
- Configure basic MLD functions.

Enabling MLD fast-leave processing

In some applications, such as ADSL dial-up networking, only one multicast receiver host is attached to an interface of the MLD querier. To allow fast response to the MLD done messages of the host when it switches frequently from one IPv6 multicast group to another, you can enable fast-leave processing on the MLD querier.

With MLD fast-leave processing enabled, after receiving an MLD done message or a MLD state change report message from a host, the MLD querier sends a leave notification to the upstream immediately without first sending MLD multicast-address-specific queries to downstream hosts. This reduces leave latency and preserves the network bandwidth.

To enable MLD fast-leave processing:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Enable MLD fast-leave processing.	**mld fast-leave** [**group-policy** *acl6-number*]	By default, the MLD fast-leave processing is disabled.

Displaying and maintaining MLD

△ CAUTION:

The **reset mld group** command might cause IPv6 multicast data transmission failures.

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display MLD group information.	**display mld** [**vpn-instance** *vpn-instance-name*] **group** [*ipv6-group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]
Display MLD information.	**display mld** [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**]
Remove all the dynamic group entries of an MLD group or all MLD groups.	**reset mld** [**vpn-instance** *vpn-instance-name*] **group** { **all** | **interface** *interface-type interface-number* { **all** | *ipv6-group-address* [*prefix-length*] [*ipv6-source-address* [*prefix-length*]] } }

NOTE:

The **reset mld group** command cannot remove static MLD group entries.

MLD configuration example

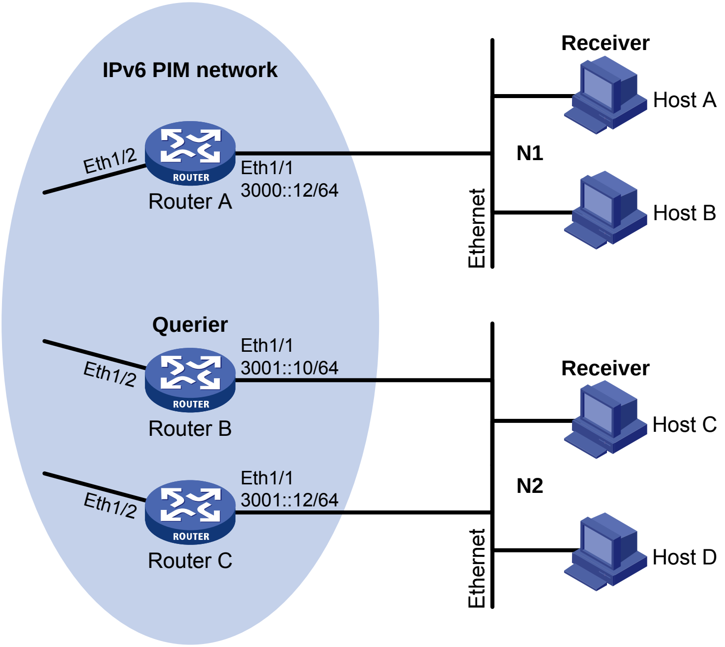
Network requirements

As shown in Figure 42, VOD streams are sent to receiver hosts in multicast. Receiver hosts of different organizations form stub networks N1 and N2. Host A and Host C are multicast receiver hosts in N1 and N2, respectively.

MLDv1 runs between Router A and N1, and between the other two routers (Router B and Router C) and N2. Router A acts as the MLD querier in N1. Router B acts as the MLD querier in N2 because it has a lower IPv6 address.

The hosts in N1 can only join the IPv6 multicast group FF1E::101. The hosts in N2 can join any IPv6 multicast groups.

Figure 42 Network diagram



Configuration procedure

1. Assign an IPv6 address and prefix length to each interface as shown in Figure 42. (Details not shown.)
2. Configure OSPFv3 between the routers on the IPv6 PIM network to make sure the network-layer is interoperable on the IPv6 PIM network and routing information among the routers can be dynamically updated. (Details not shown.)
3. Enable the IPv6 multicast routing, MLD, and IPv6 PIM-DM:

   # On Router A, enable IPv6 multicast routing globally, enable MLD on Ethernet 1/1, and enable IPv6 PIM-DM on each interface.

   ```
   <RouterA> system-view
   [RouterA] ipv6 multicast routing
   [RouterA-mrib6] quit
   ```

```
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] mld enable
[RouterA-Ethernet1/1] ipv6 pim dm
[RouterA-Ethernet1/1] quit
[RouterA] interface ethernet 1/2
[RouterA-Ethernet1/2] ipv6 pim dm
[RouterA-Ethernet1/2] quit
```

# On Router B, enable IPv6 multicast routing globally, enable MLD on Ethernet 1/1, and enable IPv6 PIM-DM on each interface.

```
<RouterB> system-view
[RouterB] ipv6 multicast routing
[RouterB-mrib6] quit
[RouterB] interface ethernet 1/1
[RouterB-Ethernet1/1] mld enable
[RouterB-Ethernet1/1] ipv6 pim dm
[RouterB-Ethernet1/1] quit
[RouterB] interface ethernet 1/2
[RouterB-Ethernet1/2] ipv6 pim dm
[RouterB-Ethernet1/2] quit
```

# On Router C, enable IPv6 multicast routing, enable MLD on Ethernet 1/1, and enable IPv6 PIM-DM on each interface.

```
<RouterC> system-view
[RouterC] ipv6 multicast routing
[RouterC-mrib6] quit
[RouterC] interface ethernet 1/1
[RouterC-Ethernet1/1] mld enable
[RouterC-Ethernet1/1] ipv6 pim dm
[RouterC-Ethernet1/1] quit
[RouterC] interface ethernet 1/2
[RouterC-Ethernet1/2] ipv6 pim dm
[RouterC-Ethernet1/2] quit
```

4. Configure an IPv6 multicast group filter on Router A, so that the hosts connected to Ethernet 1/1 can join IPv6 multicast group FF1E::101 only.

```
[RouterA] acl ipv6 number 2001
[RouterA-acl6-basic-2001] rule permit source ff1e::101 128
[RouterA-acl6-basic-2001] quit
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] mld group-policy 2001
[RouterA-Ethernet1/1] quit
```

Verifying the configuration

Display MLD information on Ethernet 1/1 of Router B.

```
[RouterB] display mld interface ethernet 1/1
 Ethernet1/1(FE80::200:5EFF:FE66:5100):
   MLD is enabled.
   MLD version: 1
   Query interval for MLD: 125s
   Other querier present time for MLD: 255s
   Maximum query response time for MLD: 10s
   Querier for MLD: FE80::200:5EFF:FE66:5100 (this router)
  MLD groups reported in total: 1
```

Troubleshooting MLD

No member information exists on the receiver-side router

Symptom

When a host sends a message to announce its joining IPv6 multicast group G, no member information of multicast group G exists on the immediate router.

Analysis

- The correctness of networking and interface connections and whether the protocol layer of the interface is up directly affect the generation of IPv6 group member information.
- IPv6 multicast routing must be enabled on the router. 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 cannot 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. Use the **display mld interface** command to verify that the networking, interface connections, and IP address configuration are correct. If the command does not produce output, the interface is in an abnormal state. The reason might be that you have configured the **shutdown** command on the interface, that the interface is not correctly connected, or that the IPv6 address configuration is not correctly done.
2. Use the **display current-configuration** command to verify that the IPv6 multicast routing is enabled. If it is not enabled, use the **ipv6 multicast routing** command in system view to enable IPv6 multicast routing. In addition, verify that MLD is enabled on the associated interfaces.
3. Use the **display mld interface** command to verify that the MLD version on the interface is lower than that on the host.
4. Use the **display current-configuration interface** command to verify that no ACL rule has been configured to filter out the reports sent by the host to the IPv6 multicast group G.

Inconsistent membership information on the routers on the same subnet

Symptom

Different memberships are maintained on different MLD routers on the same subnet.

Analysis

- A router running MLD maintains multiple parameters for each interface. Inconsistent MLD interface parameter configurations for routers on the same subnet result in inconsistent MLD memberships.
- Although routers are partially compatible with hosts that separately run different versions of MLD, all routers on the same subnet must run the same MLD version. Inconsistent MLD versions running on routers on the same subnet lead to inconsistent MLD memberships.

Solution

1. Use the **display current-configuration** command to verify the MLD information on the interface.
2. Use the **display mld interface** command on all routers on the same subnet to check the MLD timers for inconsistent configurations.
3. Use the **display mld interface** command to verify that the routers are running the same MLD version.

Configuring IPv6 PIM

PIM overview

Protocol Independent Multicast for IPv6 (IPv6 PIM) provides IPv6 multicast forwarding by leveraging IPv6 unicast static routes or IPv6 unicast routing tables generated by any IPv6 unicast routing protocol, such as RIPng, OSPFv3, IPv6 IS-IS, or IPv6 BGP. IPv6 PIM is not dependent on any particular IPv6 unicast routing protocol, and it uses the underlying IPv6 unicast routing to generate a routing table with routes.

IPv6 PIM uses the RPF mechanism to implement multicast forwarding. When an IPv6 multicast packet arrives on an interface of the device, the packet undergoes an RPF check. If the RPF check succeeds, the device creates an IPv6 multicast routing entry and forwards the packet. If the RPF check fails, the device discards the packet. For more information about RPF, see "Configuring IPv6 multicast routing and forwarding."

Based on the implementation mechanism, IPv6 PIM includes the following categories:

- Protocol Independent Multicast–Dense Mode for IPv6 (IPv6 PIM-DM)
- Protocol Independent Multicast–Sparse Mode for IPv6 (IPv6 PIM-SM)
- Protocol Independent Multicast Source-Specific Multicast for IPv6 (IPv6 PIM-SSM)

In this document, an IPv6 PIM domain refers to a network composed of IPv6 PIM routers.

IPv6 PIM-DM overview

IPv6 PIM-DM uses the push mode for multicast forwarding and is suitable for small networks with densely distributed IPv6 multicast members.

The following describes the basic implementation of IPv6 PIM-DM:

- IPv6 PIM-DM assumes that all downstream nodes want to receive IPv6 multicast data when a source starts sending, so IPv6 multicast data is flooded to all downstream nodes on the network.
- Branches without downstream receivers are pruned from the forwarding trees, leaving only those branches that contain receivers.
- The pruned state of a branch has a finite holdtime timer. When the timer expires, IPv6 multicast data is again forwarded to the pruned branch. This flood-and-prune cycle takes place periodically to maintain the forwarding branches.
- To reduce join latency when a new receiver on a previously pruned branch joins an IPv6 multicast group, IPv6 PIM-DM uses a graft mechanism to turn the pruned branch into a forwarding branch.

In IPv6 PIM-DM, the multicast forwarding paths for an IPv6 multicast group constitute a source tree, which is rooted at the IPv6 multicast source and has multicast group members as its "leaves." Because the source tree consists of the shortest paths from the IPv6 multicast source to the receivers, it is also called a "shortest path tree (SPT)."

The operating mechanism of IPv6 PIM-DM is summarized as follows:

- Neighbor discovery
- SPT building

- Graft
- Assert

Neighbor discovery

In an IPv6 PIM domain, each interface that runs IPv6 PIM on a router periodically multicasts IPv6 PIM hello messages to all other IPv6 PIM routers on the local subnet to discover IPv6 PIM neighbors, maintain IPv6 PIM neighboring relationship with other routers, and build and maintain SPTs.

SPT building

The process of building an SPT is the flood-and-prune process:

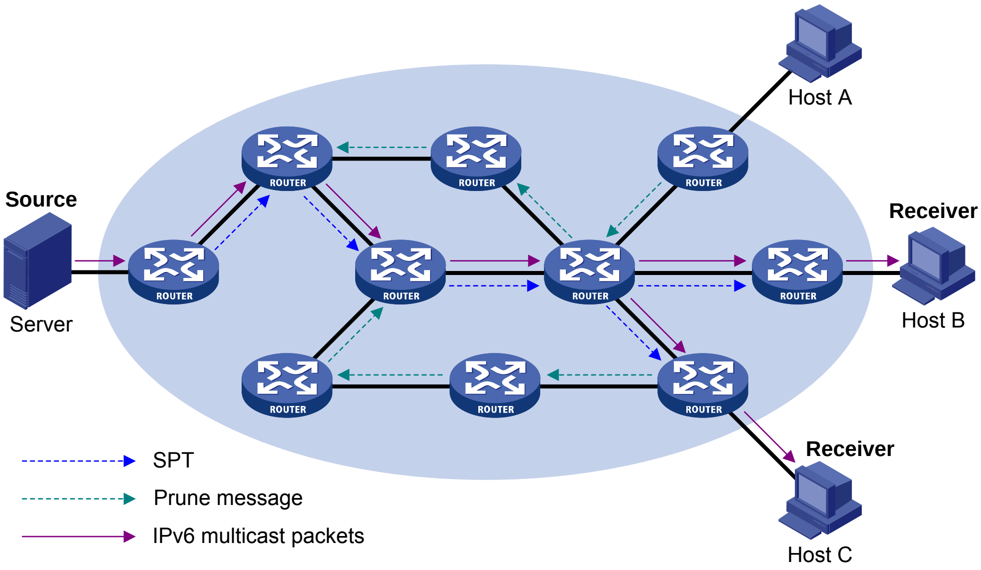
1. In an IPv6 PIM-DM domain, when the IPv6 multicast source S sends IPv6 multicast data to the IPv6 multicast group G, the IPv6 multicast data is flooded throughout the domain. A router performs an RPF check for the IPv6 multicast data. If the check succeeds, the router creates an (S, G) entry and forwards the data to all downstream nodes in the network. In the flooding process, all the routers in the IPv6 PIM-DM domain create the (S, G) entry.
2. The nodes without downstream receivers are pruned. A router that has no downstream receivers sends a prune message to the upstream node to remove the interface that receives the prune message from the (S, G) entry. In this way, the upstream stream node stops forwarding subsequent packets addressed to that IPv6 multicast group down to this node.

NOTE:

An (S, G) entry contains an IPv6 multicast source address S, an IPv6 multicast group address G, an outgoing interface list, and an incoming interface.

A prune process is initiated by a leaf router. As shown in Figure 43, the router interface that does not have any downstream receivers initiates a prune process by sending a prune message toward the IPv6 multicast source. This prune process goes on until only necessary branches are left in the IPv6 PIM-DM domain, and these necessary branches constitute an SPT.

Figure 43 SPT building



The pruned state of a branch has a finite holdtime timer. When the timer expires, IPv6 multicast data is again forwarded to the pruned branch. The flood-and-prune cycle takes place periodically to maintain the forwarding branches.

Graft

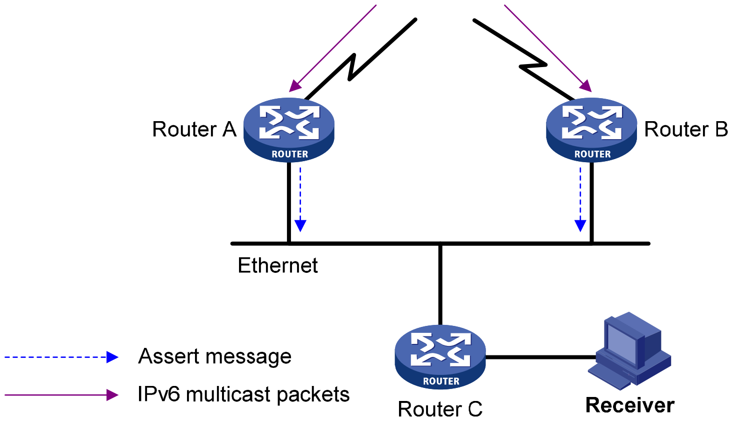
To reduce the join latency when a new receiver on a previously pruned branch joins an IPv6 multicast group, IPv6 PIM-DM uses a graft mechanism to turn the pruned branch into a forwarding branch, as follows:

1. The node that needs to receive the IPv6 multicast data sends a graft message to its upstream node, telling it to rejoin the SPT.
2. After receiving this graft message, the upstream node adds the interface that received the graft message into the outgoing interface list of the (S, G) entry for the IPv6 multicast group, and then sends 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 continues to send graft messages at a configurable interval until it receives an acknowledgment from its upstream node.

Assert

On a subnet with more than one multicast router, the assert mechanism shuts off duplicate multicast flows to the network. It does this by electing a unique multicast forwarder for the subnet.

Figure 44 Assert mechanism



As shown in Figure 44, after Router A and Router B receive an (S, G) packet from the upstream node, they both forward the packet to the local subnet. As a result, the downstream node Router C receives two identical multicast packets, and both Router A and Router B, on their own downstream interfaces, receive a duplicate packet forwarded by the other. After 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 IPv6 multicast source address (S), the IPv6 multicast group address (G), and the preference and metric of the IPv6 unicast route/MBGP route/static multicast route to the IPv6 multicast source. By comparing these parameters, either Router A or Router B becomes the unique forwarder of the subsequent (S, G) packets on the subnet. The comparison process is as follows:

1. The router with a higher preference to the IPv6 multicast source wins.
2. If both routers have the same preference to the IPv6 multicast source, the router with a smaller metric to the IPv6 multicast source wins.
3. If a tie exists in route metric to the IPv6 multicast source, the router with a higher IPv6 link-local address on the downstream interface wins.

IPv6 PIM-SM overview

IPv6 PIM-DM uses the flood-and-prune cycles to build SPTs for IPv6 multicast data forwarding. Although an SPT has the shortest paths from the IPv6 multicast source to the receivers, it is built with a low efficiency and is not suitable for large- and medium-sized networks.

IPv6 PIM-SM uses the pull mode for IPv6 multicast forwarding, and it 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 IPv6 multicast data. In the IPv6 PIM-SM mode, a host must express its interest in the IPv6 multicast data for an IPv6 multicast group before the data is forwarded to it. IPv6 PIM-SM implements multicast forwarding by building and maintaining rendezvous point trees (RPTs). An RPT is rooted at a router that has been configured as the rendezvous point (RP) for an IPv6 multicast group, and the IPv6 multicast data to the group is forwarded by the RP to the receivers along the RPT.
- When a receiver expresses its interest in the IPv6 multicast data addressed to a specific IPv6 multicast group, the receiver-side designated router (DR) sends a join message to the RP for the 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 data to an IPv6 multicast group, the source-side DR must register the IPv6 multicast source with the RP by unicasting register messages to the RP. The IPv6 multicast source stops sending register message until it receives a register-stop message from the RP. When the RP receives the register message, it triggers the establishment of an SPT. Then, the IPv6 multicast source sends subsequent IPv6 multicast packets along the SPT to the RP. After reaching the RP, the multicast packet is duplicated and delivered to the receivers along the RPT.

Multicast data is replicated wherever the RPT branches, and this process automatically repeats until the IPv6 multicast data reaches the receivers.

The operating mechanism of IPv6 PIM-SM is summarized as follows:

- Neighbor discovery
- DR election
- RP discovery
- Embedded RP
- RPT building
- IPv6 multicast source registration
- Switchover to SPT
- Assert

Neighbor discovery

IPv6 PIM-SM uses a similar neighbor discovery mechanism as IPv6 PIM-DM does. For more information, see "Neighbor discovery."

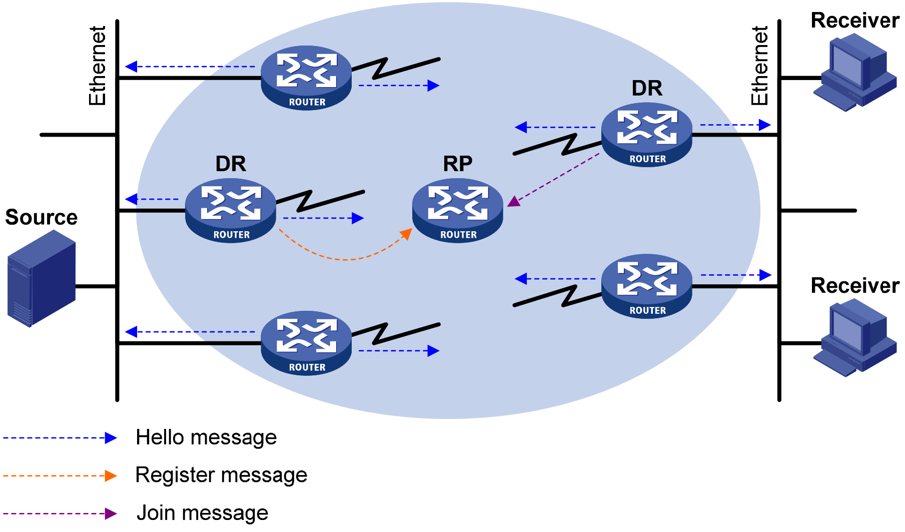
DR election

On a shared-media LAN like Ethernet, only a DR forwards IPv6 multicast data. A DR is required in both the source-side network and receiver-side network. A source-side DR acts on behalf of the IPv6 multicast source to sends register messages to the RP, and the receiver-side DR acts on behalf of the receiver hosts to sends join messages to the RP.

IMPORTANT:

MLD must be enabled on the device that acts as the receiver-side DR. Otherwise, the receiver hosts attached to the DR cannot join any IPv6 multicast groups. For more information about MLD, see "Configuring MLD."

Figure 45 DR election



As shown in Figure 45, the DR election process is as follows:

1. The routers on the shared-media LAN send hello messages to one another. The hello messages contain the priority for DR election. The router with the highest DR priority is elected as the DR.
2. In the case of a tie in the 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 wins the DR election.

If the DR fails, its IPv6 PIM neighbor lifetime expires, and the other routers initiate a new DR election.

RP discovery

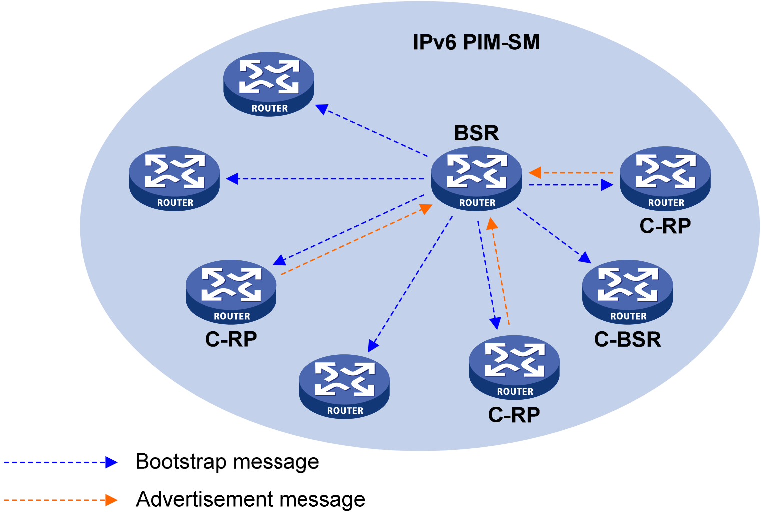
An RP is the core of an IPv6 PIM-SM domain. For a small-sized, simple network, one RP is enough for multicast forwarding throughout the network. In this case, you can specify a static RP on each router in the IPv6 PIM-SM domain. However, in an IPv6 PIM-SM network that covers a wide area, a huge amount of IPv6 multicast data is forwarded by the RP. To lessen the RP burden and optimize the topological structure of the RPT, you can configure multiple candidate-RPs (C-RPs) in an IPv6 PIM-SM domain and use the bootstrap mechanism to dynamically elect RPs. An elected RP provides services for a different IPv6 multicast group. For this purpose, you must configure a bootstrap router (BSR). A BSR serves as the administrative core of an IPv6 PIM-SM domain. An IPv6 PIM-SM domain has only one BSR, but can have multiple candidate-BSRs (C-BSRs) so that, if the BSR fails, a new BSR can be automatically elected from the C-BSRs and avoid service interruption.

NOTE:

- An RP can provide services for multiple IPv6 multicast groups, but an IPv6 multicast group only uses one RP.
- A device can act as a C-RP and a C-BSR at the same time.

As shown in Figure 46, each C-RP periodically unicasts its advertisement messages (C-RP-Adv messages) to the BSR. An advertisement message contains the address of the advertising C-RP and the IPv6 multicast group range to which it is designated. The BSR collects these advertisement messages and organizes the C-RP information into an RP-set, which is a database of mappings between IPv6 multicast groups and RPs. The BSR encapsulates the RP-set information in the bootstrap messages (BSMs) and floods the BSMs to the entire IPv6 PIM-SM domain.

Figure 46 Information exchange between C-RPs and BSR



Based on the information in the RP-set, all routers in the network can select the proper RP for a specific IPv6 multicast group based on the following rules:

1. The C-RP with the highest priority wins.
2. If all the C-RPs have the same priority, the C-RP with the largest hash value (calculated through the hash algorithm) wins.
3. If all the C-RPs have the same priority and hash value, the C-RP with the highest IPv6 address wins.

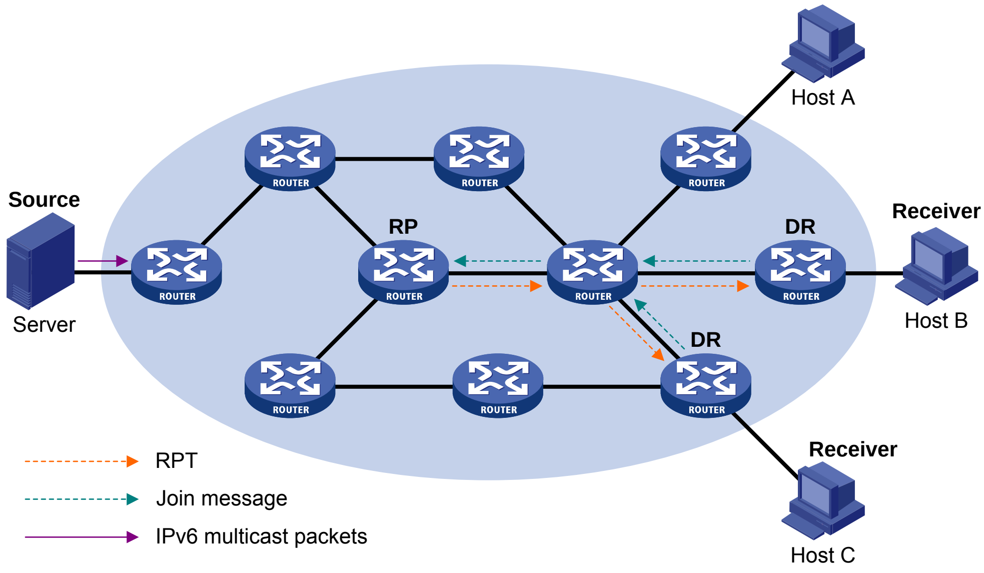
Embedded RP

The embedded RP mechanism enables a router to resolve the RP address from an IPv6 multicast group address to map the IPv6 multicast group to an RP. This RP can take the place of the configured static RP or the RP dynamically elected by the bootstrap mechanism. A DR does not need to learn the RP address beforehand. The process is as follows:

- At the receiver side:
  a. A receiver host initiates an MLD report to express its interest in an IPv6 multicast group.
  b. After receiving the MLD report, the receiver-side DR resolves the RP address embedded in the IPv6 multicast group address and sends a join message to the RP.
- At the IPv6 multicast source side:
  c. The IPv6 multicast source sends IPv6 multicast traffic to an IPv6 multicast group.
  d. The source-side DR resolves the RP address embedded in the IPv6 multicast address, and sends a register message to the RP.

RPT building

Figure 47 RPT building in an IPv6 PIM-SM domain



As shown in Figure 47, the process of building an RPT is as follows:

1. When a receiver wants to join the IPv6 multicast group G, it uses an MLD message to inform the receiver-side DR.
2. After getting the receiver information, the DR sends a join message, which is forwarded hop by hop to the RP for the IPv6 multicast group.
3. The routers along the path from the DR to the RP form an RPT branch. Each router on this branch adds to its forwarding table a (*, G) entry, where the asterisk (*) means any IPv6 multicast source. The RPT is rooted at the RP and has the DR as its leaf.

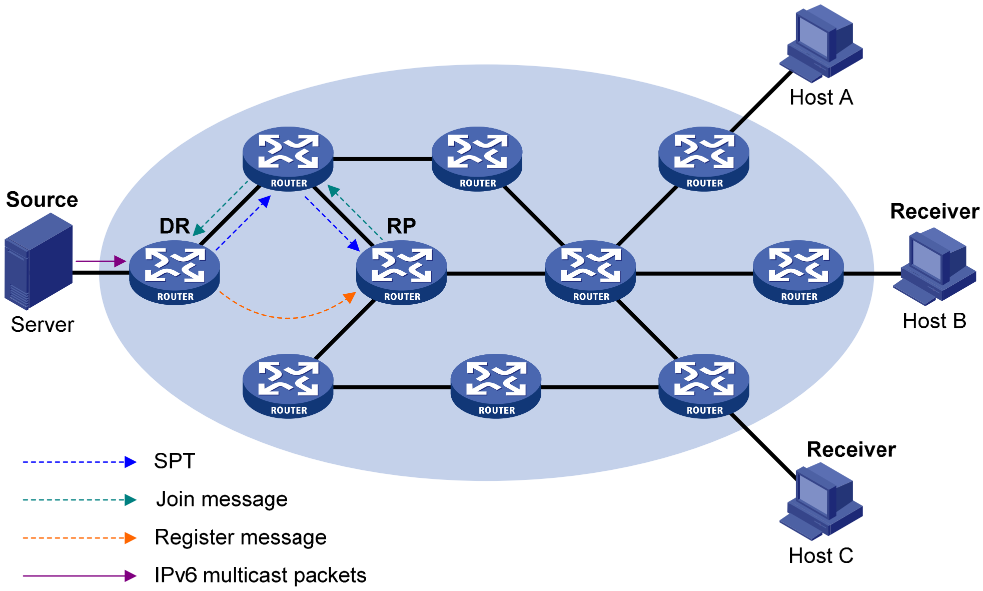
When the IPv6 multicast data addressed to the IPv6 multicast group G reaches the RP, the RP forwards the data to the DR along the established RPT, and finally to the receiver.

When a receiver is no longer interested in the IPv6 multicast data addressed to the IPv6 multicast group G, the receiver-side DR sends a prune message, which goes hop by hop along the RPT to the RP. After receiving the prune message, the upstream node deletes the interface that connects to this downstream node from the outgoing interface list and checks whether it has receivers for that IPv6 multicast group. If not, the router continues to forward the prune message to its upstream router.

IPv6 multicast source registration

The IPv6 multicast source uses the registration process to inform an RP of its presence.

Figure 48 IPv6 multicast source registration



As shown in Figure 48, the IPv6 multicast source registers with the RP as follows:

1. The IPv6 multicast source S sends the first multicast packet to the IPv6 multicast group G. When receiving the multicast packet, the source-side DR that directly connects to the IPv6 multicast source encapsulates the packet in an register message and unicasts the message to the RP.
2. After the RP receives the register message, it decapsulates it and forwards it down to the RPT. Meanwhile, it sends an (S, G) source-specific join message hop by hop toward the IPv6 multicast source. The routers along the path from the RP to the IPv6 multicast source constitute an SPT branch, and each router on this branch creates an (S, G) entry in its forwarding table. The SPT is rooted at the source-side DR, and has the RP as its leaf.
3. The subsequent IPv6 multicast data from the IPv6 multicast source are forwarded to the RP along the established branch, and the RP forwards the data to the receivers along the RPT. When the IPv6 multicast data reaches the RP along the SPT, the RP unicasts a register-stop message to the source-side DR to prevent the DR from unnecessarily encapsulating the data.

Switchover to SPT

△ CAUTION:

If the router is an RP, disabling switchover to SPT might cause multicast traffic forwarding failures on the source-side DR. When disabling switchover to SPT, be sure you fully understand its impact on your network.

In an IPv6 PIM-SM domain, only one RP and one RPT provide services for a specific IPv6 multicast group. Before the switchover to SPT occurs, the source-side DR encapsulates all IPv6 multicast data addressed to the IPv6 multicast group in register messages and sends them to the RP. After receiving these register messages, the RP decapsulates them and forwards them to the receivers-side DR along the RPT.

Switchover to SPT has the following weaknesses:

- Encapsulation and decapsulation are complex on the source-side DR and the RP.
- The path for an IPv6 multicast packet might not be the shortest one.
- The RP might be overloaded by IPv6 multicast traffic bursts.

To eliminate these weaknesses, IPv6 PIM-SM allows an RP or the receiver-side DR to initiate a switchover to SPT when the traffic rate exceeds a specific threshold:

- The RP initiates a switchover to SPT:

  The RP periodically checks the multicast packet forwarding rate. If the RP finds that the traffic rate exceeds the specified threshold, it sends an (S, G) source-specific join message hop by hop toward the IPv6 multicast source. The routers along the path from the RP to the IPv6 multicast source constitute an SPT branch. The subsequent IPv6 multicast data for the IPv6 multicast group can be forwarded to the RP along the branch without being encapsulated in register messages.

  For more information about the switchover to SPT initiated by the RP, see "IPv6 multicast source registration."
- The receiver-side DR initiates a switchover to SPT:

  The receiver-side DR periodically checks the forwarding rate for the multicast packets that the IPv6 multicast source S sends to the IPv6 multicast group G. If the forwarding rate exceeds the specified threshold, the DR initiates a switchover to SPT, as follows:

  a. The receiver-side DR sends an (S, G) source-specific join message hop by hop toward the IPv6 multicast source. The routers along the path from the RP to the source-side DR create an (S, G) entry in their forwarding table to constitute an SPT branch.
  b. When the multicast packets for the IPv6 multicast group are forwarded to the router where the RPT and the SPT branches, the router drops the multicast packets that reach it along the RPT and sends a prune message with the RP bit hop by hop to the RP. After receiving the prune message, the RP forwards it toward the IPv6 multicast source (supposed only one receiver exists). Thus, the switchover to SPT is completed.
  c. Finally, the IPv6 multicast source sends the multicast packets for the IPv6 multicast group to the receiver along the SPT.

With the switchover to SPT, IPv6 PIM-SM builds SPTs more economically than IPv6 PIM-DM does.

Assert

IPv6 PIM-SM uses a similar assert mechanism as IPv6 PIM-DM does. For more information, see "Assert."

IPv6 administrative scoping overview

Typically, an IPv6 PIM-SM domain contains only one BSR, which is responsible for advertising RP-set information within the entire IPv6 PIM-SM domain. Information about all IPv6 multicast groups is forwarded within the network that the BSR administers. This is called the "IPv6 non-scoped BSR mechanism."

IPv6 administrative scoping mechanism

To implement refined management, you can divide an IPv6 PIM-SM domain into an IPv6 global-scoped zone and multiple IPv6 administratively-scoped zones (admin-scoped zones). This is called the "IPv6 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.

An IPv6 admin-scoped zone is designated to particular IPv6 multicast groups with the same scope field value in their group addresses. Zone border routers (ZBRs) form the boundary of an IPv6 admin-scoped zone. Each IPv6 admin-scoped zone maintains one BSR for IPv6 multicast groups with the same scope field value. IPv6 multicast protocol packets, such as assert messages and BSMs, of these IPv6 multicast groups cannot cross the boundary of the IPv6 admin-scoped zone for the group range. The IPv6 multicast group ranges to which different IPv6 admin-scoped zones are designated can have intersections, but the IPv6 multicast groups in an IPv6 admin-scoped zone are valid only within its local zone, and theses IPv6 multicast groups are regarded as private group addresses.

The IPv6 global-scoped zone can be regarded as a special IPv6 admin-scoped zone, and it maintains a BSR for the IPv6 multicast groups with the scope field value as 14.

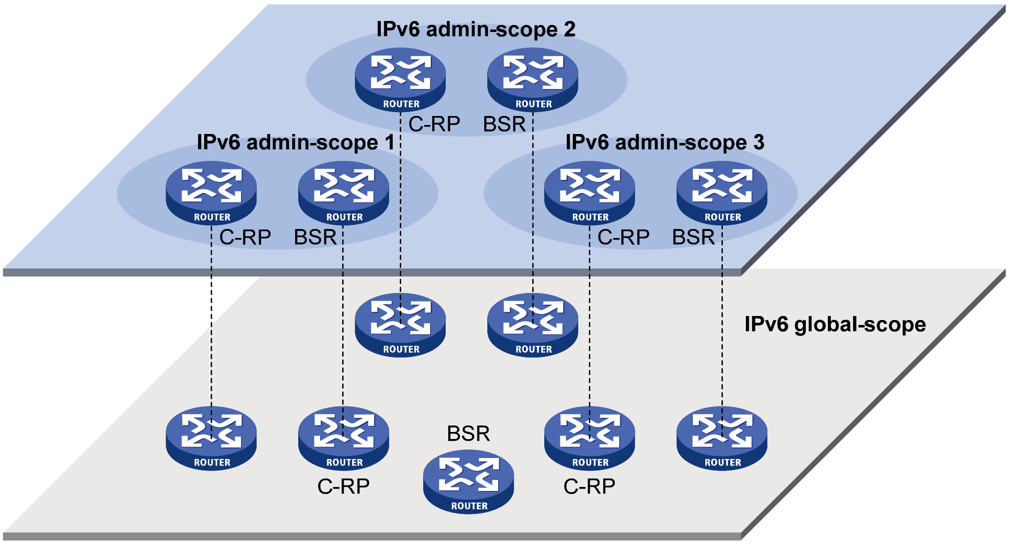
Relationship between IPv6 admin-scoped zones and the IPv6 global-scoped zone

The IPv6 global-scoped zone and each IPv6 admin-scoped zone have their own C-RPs and BSRs. These devices take effect only on their respective zones, and the BSR election and the RP election are implemented independently. Each IPv6 admin-scoped zone has its own boundary. The IPv6 multicast information within a zone cannot cross this boundary in either direction. You can have a better understanding of the IPv6 global-scoped zone and IPv6 admin-scoped zones based on geographical locations and the scope field values.

- In view of geographical locations

  An IPv6 admin-scoped zone is a logical zone for particular IPv6 multicast groups with the same scope filed value. The IPv6 multicast packets for such IPv6 multicast groups are confined within the local IPv6 admin-scoped zone and cannot cross the boundary of the zone.

  Figure 49 Relationship in view of geographical locations

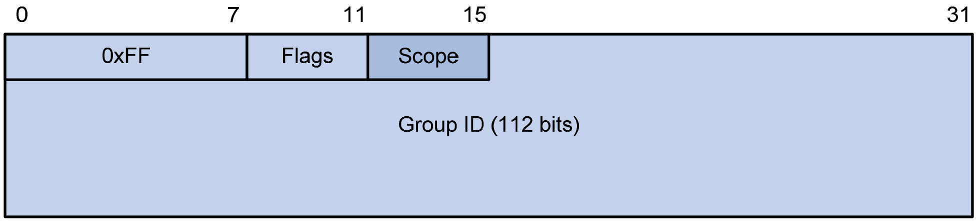


  As shown in Figure 49, for the IPv6 multicast groups with the same scope field value, the IPv6 admin-scoped zones must be geographically separated and isolated. The IPv6 global-scoped zone includes all routers in the IPv6 PIM-SM domain. IPv6 multicast packets that do not belong to any IPv6 admin-scoped zones are forwarded in the entire IPv6 PIM-SM domain.

- In view of the scope field values

  In terms of the scope field values, the scope field in an IPv6 multicast group address shows the zone to which the IPv6 multicast group belongs.

Figure 50 IPv6 multicast address format



An IPv6 admin-scoped zone with a larger scope field value contains an IPv6 admin-scoped zone with a smaller scope field value. The zone with the scope field value of E is the IPv6 global-scoped zone. Table 6 lists the possible values of the scope field.

Table 6 Values of the Scope field

Value	Meaning	Remarks
0, F	Reserved	N/A
1	Interface-local scope	N/A
2	Link-local scope	N/A
3	Subnet-local scope	IPv6 admin-scoped zone.
4	Admin-local scope	IPv6 admin-scoped zone.
5	Site-local scope	IPv6 admin-scoped zone.
6, 7, 9 through D	Unassigned	IPv6 admin-scoped zone.
8	Organization-local scope	IPv6 admin-scoped zone.
E	Global scope	IPv6 global-scoped zone.

IPv6 PIM-SSM overview

The ASM model includes IPv6 PIM-DM and IPv6 PIM-SM. The SSM model can be implemented by leveraging part of the IPv6 PIM-SM technique. It is also called "IPv6 PIM-SSM."

The SSM model provides a solution for source-specific multicast. It maintains the relationship between hosts and routers through MLDv2.

In actual applications, part of MLDv2 and IPv6 PIM-SM techniques are adopted to implement the SSM model. In the SSM model, because receivers have located an IPv6 multicast source, no RP or RPT is required, and no source registration process is required for discovering IPv6 multicast sources in other IPv6 PIM domains.

The operating mechanism of IPv6 PIM-SSM is summarized as follows:

- Neighbor discovery
- DR election
- SPT building

Neighbor discovery

IPv6 PIM-SSM uses the same neighbor discovery mechanism as IPv6 PIM-SM. For more information, see "Neighbor discovery."

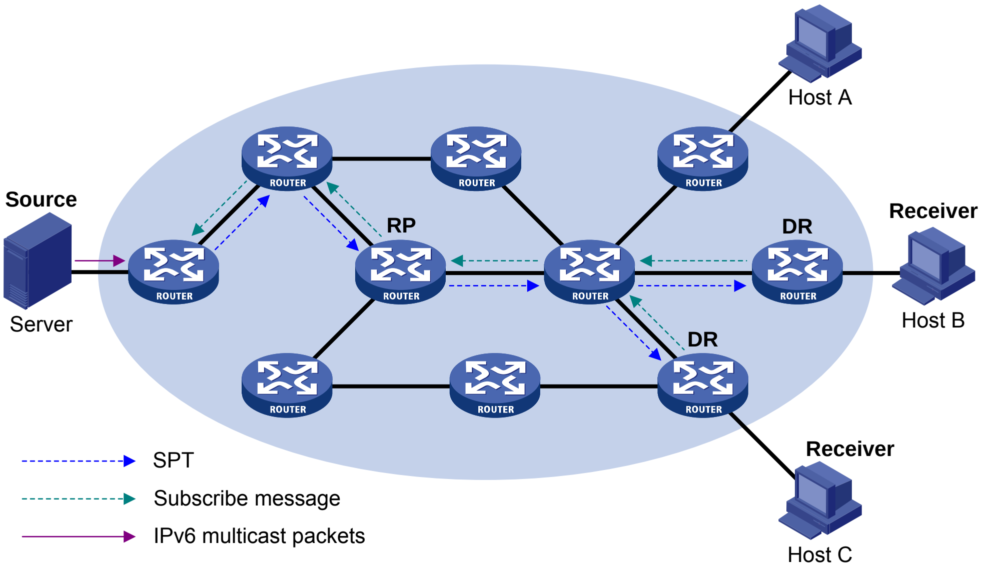
DR election

IPv6 PIM-SSM uses the same DR election mechanism as IPv6 PIM-SM. For more information, see "DR election."

SPT building

The decision to build an RPT for IPv6 PIM-SM or an SPT for IPv6 PIM-SSM depends on whether the IPv6 multicast group that the receiver wants to join is included in the IPv6 SSM group range (FF3x::/32 reserved by IANA, where "x" represents any legal address scope).

Figure 51 SPT building in IPv6 PIM-SSM



As shown in Figure 51, Host B and Host C are receivers. They send MLDv2 report messages to their DRs to express their interest in the multicast information that the IPv6 multicast source S sends to the IPv6 multicast group G.

After receiving a report message, the DR first checks whether the group address in the message is in the IPv6 SSM group range and does the following:

- If the group address is in the IPv6 SSM group range, the DR sends a subscribe message hop by hop toward the IPv6 multicast source S. All routers along the path from the DR to the IPv6 multicast source create an (S, G) entry so as to build an SPT, which is rooted the IPv6 multicast source S and has the receivers as its leaves. This SPT is the transmission channel in IPv6 PIM-SSM.
- If the group address is not in the IPv6 SSM group range, the receiver-side DR sends a (*, G) join message to the RP, and the IPv6 multicast source registers with the source-side DR.

In IPv6 PIM-SSM, the term "channel" refers to an IPv6 multicast group, and the term "subscribe message" refers to a join message.

IPv6 PIM support for VPNs

To support IPv6 PIM for VPNs, a multicast router that runs IPv6 PIM maintains an independent set of IPv6 PIM neighbor table, IPv6 multicast routing table, BSR information, and RP-set information for each VPN.

After receiving an IPv6 multicast data packet, the multicast router checks which VPN the IPv6 data packet belongs to, and then forwards the IPv6 packet according to the IPv6 multicast routing table for that VPN or creates an IPv6 multicast routing entry for that VPN.

Protocols and standards

- RFC 3973, *Protocol Independent Multicast-Dense Mode (PIM-DM): Protocol Specification(Revised)*
- RFC 4601, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)*
- RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*
- 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

This section describes how to configure IPv6 PIM-DM.

IPv6 PIM-DM configuration task list

Task at a glance
(Required.) Enabling IPv6 PIM-SM
(Optional.) Enabling the state refresh feature
(Optional.) Configuring state refresh parameters
(Optional.) Configuring IPv6 PIM-DM graft retry timer
(Optional.) Configuring common IPv6 PIM features

Configuration prerequisites

Before you configure IPv6 PIM-DM, configure an IPv6 unicast routing protocol so that all devices in the domain are interoperable at the network layer.

Enabling IPv6 PIM-DM

Enable IPv6 multicast routing before configuring IPv6 PIM.

With IPv6 PIM-DM enabled on interfaces, routers can establish IPv6 PIM neighbor relationship and process IPv6 PIM messages from their IPv6 PIM neighbors. When you deploy an IPv6 PIM-DM domain, enable IPv6 PIM-DM on all non-border interfaces of routers.

IMPORTANT:

All the interfaces on a device must operate in the same IPv6 PIM mode in the public network or the same VPN instance.

To enable IPv6 PIM-DM:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable IPv6 multicast routing and enter IPv6 MRIB view.	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	By default, IPv6 multicast routing is disabled.
3.	Return to system view.	**quit**	
4.	Enter interface view.	**interface** *interface-type interface-number*	N/A
5.	Enable IPv6 PIM-DM.	**ipv6 pim dm**	By default, IPv6 PIM-DM is disabled.

Enabling the state refresh feature

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 shared-media subnet can have the state refresh feature only if the state refresh feature is enabled on all IPv6 PIM routers on the subnet.

To enable the state refresh feature on all routers in IPv6 PIM-DM domain:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter interface view.	**interface** *interface-type interface-number*	N/A
3.	Enable the state refresh feature.	**ipv6 pim state-refresh-capable**	By default, the state refresh feature is enabled.

Configuring state refresh parameters

The router directly connected with the IPv6 multicast source periodically sends state refresh messages. You can configure the interval for sending such messages on that router.

A router might receive duplicate state refresh messages within a short time. To prevent this situation, you can configure the amount of time that the router must wait before receiving the next state refresh message. If the router receives a new state refresh message within the specified waiting time, it discards it. If this timer times out, the router accepts a new state refresh message, refreshes its own IPv6 PIM-DM state, and resets 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, configure an appropriate hop limit value based on the network size on the router directly connected with the IPv6 multicast source.

To configure state refresh parameters:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter IPv6 PIM view.	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure the interval to send state refresh messages.	**state-refresh-interval** *interval*	By default, the interval to send refresh messages is 60 seconds.
4.	Configure the time to wait before receiving a new state refresh message.	**state-refresh-rate-limit** *time*	By default, the waiting time is 30 seconds.
5.	Configure the hop limit value of state refresh messages.	**state-refresh-hoplimit** *hoplimit-value*	By default, the hop limit value of state refresh messages is 255.

Configuring IPv6 PIM-DM graft retry timer

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 (graft retry timer) until it receives a graft-ack message from the upstream router. For more information about the configuration of other timers in IPv6 PIM-DM, see "Configuring common IPv6 PIM timers."

To configure the IPv6 PIM-DM graft retry timer:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure the graft retry timer.	**ipv6 pim timer graft-retry** *interval*	By default, the graft retry timer is 3 seconds.

Configuring IPv6 PIM-SM

IPv6 PIM-SM configuration task list

Task at a glance
(Required.) Enabling IPv6 PIM-SM
(Required.) Configuring an RP: • Configuring a static RP • Configuring a C-RP NOTE: Perform at least one of the tasks. In a network with a static RP, skip the task of configuring a BSR.
Configure a BSR:

Task at a glance
• (Required.) Configuring a C-BSR • (Optional.) Configuring an IPv6 PIM domain border • (Optional.) Disabling the BSM semantic fragmentation function
(Optional.) Configuring IPv6 multicast source registration
(Optional.) Configuring switchover to SPT
(Optional.) Configuring common IPv6 PIM features

Configuration prerequisites

Before you configure IPv6 PIM-SM, configure an IPv6 unicast routing protocol so that all devices in the domain are interoperable at the network layer.

Enabling IPv6 PIM-SM

Enable IPv6 multicast routing before configuring IPv6 PIM.

With IPv6 PIM-SM enabled on interfaces, routers can establish IPv6 PIM neighbor relationship and process IPv6 PIM messages from their IPv6 PIM neighbors. When you deploy an IPv6 PIM-SM domain, HP recommends enabling IPv6 PIM-SM on all non-border interfaces.

IMPORTANT:

All the interfaces on the same router must operate in the same IPv6 PIM mode in the public network or the same VPN instance.

To enable IPv6 PIM-SM:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable IPv6 multicast routing and enter IPv6 MRIB view.	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	By default, IPv6 multicast routing is disabled.
3. Return to system view.	**quit**	
4. Enter interface view.	**interface** *interface-type interface-number*	N/A
5. Enable IPv6 PIM-SM.	**ipv6 pim sm**	By default, IPv6 PIM-SM is disabled.

Configuring an RP

An RP can provide services for multiple or all IPv6 multicast groups. However, only one RP can forward IPv6 multicast traffic for an IPv6 multicast group at a moment.

An RP can be manually configured or dynamically elected through the BSR mechanism. For a large-scaled IPv6 PIM network, configuring static RPs is a tedious job. Generally, static RPs are backups for dynamic RPs to enhance the robustness and operational manageability on an IPv6 multicast network.

Configuring a static RP

If only one dynamic RP exists on a network, you can configure a static RP to avoid communication interruption caused by single-point failures. It can also avoid waste of bandwidth due to frequent message exchange between C-RPs and the BSR. The static RP configuration must be the same on all routers in the IPv6 PIM-SM domain.

To configure a static RP:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter IPv6 PIM view.	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure a static RP for IPv6 PIM-SM.	**static-rp** *ipv6-rp-address* [*acl6-number* | **preferred**] *	By default, no static RP is configured.

Configuring a C-RP

In an IPv6 PIM-SM domain, if you want a router to become the RP, you can configure the router as a C-RP. The BSR collects the C-RP information according to the received advertisement messages from C-RPs or the auto-RP announcements from other routers, and organizes the C-RP information into the RP-set information, which is flooded throughout the entire network. Then, the other routers in the network can determine the RPs for different IPv6 multicast group ranges based on the RP-set information. HP recommends configuring C-RPs on backbone routers.

To enable the BSR to distribute the RP-set information in the PIM-SM domain, the C-RPs must periodically send advertisement messages to the BSR. The BSR learns the C-RP information, encapsulates the C-RP information and its own IPv6 address in a BSM, and floods the BSM to all IPv6 PIM routers in the domain.

An advertisement message contains a holdtime option, which defines the C-RP lifetime for the advertising C-RP. After the BSR receives an advertisement message from a C-RP, it starts a timer for the C-RP. If the BSR does not receive any advertisement message when the timer expires, it regards the C-RP failed or unreachable.

To guard against C-RP spoofing, you must configure a legal C-RP address range and the multicast group range to which the C-RP is designated. In addition, because every C-BSR might become the BSR, you must configure the same filtering policy on all C-BSRs in the IPv6 PIM-SM domain.

When you configure a C-RP, reserve a relatively large bandwidth between the C-RP and the other devices in the IPv6 PIM-SM domain.

To configure a C-RP:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter IPv6 PIM view.	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure a C-RP.	**c-rp** *ipv6-address* [**advertisement-interval** *adv-interval* | { **group-policy** *acl6-number* | **scope** *scope-id* } | **holdtime** *hold-time* | **priority** *priority*] *	By default, no C-RP is configured.

Step	Command	Remarks
4. (Optional.) Configure a legal C-RP address range and the IPv6 multicast group range to which the C-RP is designated.	**crp-policy** *acl6-number*	By default, no restrictions are defined.

Configuring a BSR

You must configure a BSR if C-RPs are configured to dynamically select the RP. In a network with a static RP, this configuration task is unnecessary.

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

C-BSRs should be configured on routers on the backbone network. The BSR election process is summarized as follows:

- Initially, each C-BSR regards itself as the BSR of the IPv6 PIM-SM domain send BSMs to other routers in the domain.
- When a C-BSR receives the BSM from another C-BSR, it compares its own priority with the priority carried in the message. The C-BSR with a higher priority wins the BSR election. If a tie exists in the priority, the C-BSR with a higher IPv6 address wins. The loser uses the winner's BSR address to replace its own BSR address and no longer regards itself as the BSR, and the winner retains its own BSR address and continues to regard itself as the BSR.

In an IPv6 PIM-SM domain, the BSR collects C-RP information from the received advertisement messages from the C-RPs, encapsulates the C-RP information in the RP-set information, and distributes the RP-set information to all routers in the IPv6 PIM-SM domain. All routers use the same hash algorithm to get an RP for a specific IPv6 multicast group.

Configuring a legal BSR address range enables filtering of BSMs based on the address range, thereby preventing a maliciously configured host from masquerading as a BSR. The same configuration must be made on all routers in the IPv6 PIM-SM domain. The following describes the typical BSR spoofing cases and the corresponding preventive measures:

- Some maliciously configured hosts can forge BSMs to fool routers and change RP mappings. Such attacks often occur on border routers. Because a BSR is inside the network whereas hosts are outside the network, you can protect a BSR against attacks from external hosts by enabling the border routers to perform neighbor checks and RPF checks on BSMs and to discard unwanted messages.
- When an attacker controls a router in the network or when an illegal router is present in the network, the attacker can configure the router as a C-BSR and make it win the BSR election to advertise RP information in the network. After a router is configured as a C-BSR, it automatically floods the network with BSMs. Because a BSM has a hop limit value of 1, the whole network will not be affected as long as the neighbor router discards these BSMs. Therefore, with a legal BSR address range configured on all routers in the network, all these routers can discard BSMs from out of the legal address range.

These preventive measures can partially protect the BSR in a network. However, if an attacker controls a legal BSR, the problem still exists.

When you configure a C-BSR, reserve a relatively large bandwidth between the C-BSR and the other devices in the IPv6 PIM-SM domain.

To configure a C-BSR:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter IPv6 PIM view.	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	N/A
3. Configure a C-BSR.	**c-bsr** *ipv6-address* [**scope** *scope-id*] [**hash-length** *hash-length* | **priority** *priority*] *	By default, no C-BSR is configured.
4. (Optional.) Configure a legal BSR address range.	**bsr-policy** *acl6-number*	By default, no restrictions are defined.

Configuring an IPv6 PIM domain border

As the administrative core of an IPv6 PIM-SM domain, the BSR sends the collected RP-set information in the form of bootstrap messages to all routers in the IPv6 PIM-SM domain.

An IPv6 PIM domain border is a bootstrap message boundary. Each BSR has its specific service scope. IPv6 PIM domain border interfaces partition a network into different IPv6 PIM-SM domains. Bootstrap messages cannot cross a domain border in either direction.

Perform the following configuration on routers that you want to configure as an IPv6 PIM domain border.

To configure an IPv6 PIM border domain:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Configuring an IPv6 PIM domain border.	**ipv6 pim bsr-boundary**	By default, no IPv6 PIM domain border is configured.

Disabling the BSM semantic fragmentation function

Generally, a BSR periodically advertises the RP-set information in BSMs within the IPv6 PIM-SM domain. It encapsulates a BSM in an IPv6 datagram and might fragment the datagram if the message exceeds the MTU. In this case, 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 BSM fragments (BSMFs).

- If the RP-set information for an IPv6 multicast group range is carried in one BSMF, a non-BSR router directly updates the RP-set information for the group range after receiving the BSMF.
- If the RP-set information for an IPv6 multicast group range is carried in multiple BSMFs, a non-BSR router updates the RP-set information for the group range after receiving all these BSMFs. Because the RP-set information contained in each segment is different, loss of some IP fragments does not result in dropping of the entire BSM.

The BSM semantic fragmentation function is enabled by default. A device that does not support this function might regard a fragment as a BSM and thus learns only part of the RP-set information. Therefore, if such devices exist in the IPv6 PIM-SM domain, you must disable the BSM semantic fragmentation function on the C-BSRs.

To disable the BSM semantic fragmentation function:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter IPv6 PIM view.	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Disable the BSM semantic fragmentation function.	**undo bsm-fragment enable**	By default, BSM semantic fragmentation is enabled.

NOTE:

Generally, a BSR performs BSM semantic fragmentation according to the MTU of its BSR interface. However, for BSMs originated due to learning of a new IPv6 PIM neighbor, semantic fragmentation is performed according to the MTU of the interface that sends the BSMs.

Configuring IPv6 multicast source registration

In an IPv6 PIM-SM domain, the source-side DR sends register messages to the RP, and these register messages have different IPv6 multicast source or IPv6 multicast group addresses. You can configure a filtering rule to filter register messages so that the RP can provide services for specific IPv6 multicast groups. If the filtering rule denies an (S, G) entry, or if the filtering rule does not define an action for this entry, the RP sends a register-stop message to the DR to stop the registration process for the IPv6 multicast data.

In view of information integrity of a register message in the transmission process, you can configure the device to calculate the checksum based on the entire register message. However, to reduce the workload of encapsulating data in register messages and for the sake of interoperability, do not use this checksum calculation method.

To configure IPv6 multicast source registration:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter IPv6 PIM view.	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure a filtering rule for register messages.	**register-policy** *acl6-number*	By default, no register filtering rule exists.
4.	Configure the device to calculate the checksum based on the entire register message.	**register-whole-checksum**	By default, the device calculates the checksum based on the header of a register message.

Configuring switchover to SPT

△ CAUTION:

If the router is an RP, disabling switchover to SPT might cause multicast traffic forwarding failures on the source-side DR. When disabling switchover to SPT, be sure you fully understand its impact on your network.

Both the receiver-side DR and RP can monitor the traffic rate of passing-by IPv6 multicast packets and thus trigger a switchover from RPT to SPT.

To configure switchover to SPT:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter IPv6 PIM view.	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	N/A
3.	Configure the criteria for triggering a switchover to SPT.	**spt-switch-threshold** { *traffic-rate* | **immediacy** | **infinity** } [**group-policy** *acl6-number*]	By default, the device immediately triggers a switchover to SPT after receiving the first multicast packet.

Configuring IPv6 PIM-SSM

IPv6 PIM-SSM requires MLDv2 support. Enable MLDv2 on IPv6 PIM routers that connect to multicast receivers.

IPv6 PIM-SSM configuration task list

Task	Remarks
Enabling IPv6 PIM-SM	Required.
Configuring the IPv6 SSM group range	Optional.
Configuring common IPv6 PIM features	Optional.

Configuration prerequisites

Before you configure IPv6 PIM-SSM, configure an IPv6 unicast IPv6 routing protocol so that all devices in the domain are interoperable at the network layer.

Enabling IPv6 PIM-SM

The implementation of the IPv6 SSM model is based on subsets of IPv6 PIM-SM. Therefore, you must enable IPv6 PIM-SM before configuring IPv6 PIM-SSM.

When you deploy an IPv6 PIM-SSM domain, enable IPv6 PIM-SM on non-border interfaces of the routers.

IMPORTANT:

All the interfaces on a device must be enabled with the same IPv6 PIM mode.

To enable IPv6 PIM-SM:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable IP multicast routing, and enter MRIB view.	**ipv6 multicast routing** [**vpn-instance** *vpn-instance-name*]	By default, IPv6 multicast routing is disabled.
3. Return to system view.	**quit**	N/A
4. Enter interface view.	**interface** *interface-type interface-number*	N/A
5. Enable IPv6 PIM-SM.	**ipv6 pim sm**	By default, IPv6 PIM-SM is disabled.

Configuring the IPv6 SSM group range

When an IPv6 PIM-SM enabled interface receives an IPv6 multicast packet, it checks whether the Ipv6 multicast group address of the packet is in the IPv6 SSM group range. If the IPv6 multicast group address is in this range, the IPv6 PIM mode for this packet is IPv6 PIM-SSM. If the IPv6 multicast group address is not in this range, the IPv6 PIM mode is IPv6 PIM-SM.

Configuration guidelines

- Perform the following configuration on all routers in the IPv6 PIM-SSM domain.
- Make sure the same IPv6 SSM group range is configured on all routers in the entire domain. Otherwise, IPv6 multicast information cannot be delivered through the IPv6 SSM model.
- When a member of an IPv6 multicast group in the IPv6 SSM group range sends an MLDv1 report message, the device does not trigger a (*, G) join.

Configuration procedure

To configure an IPv6 SSM group range:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter IPv6 PIM view.	**ipv6 pim**	N/A
3. Configure the IPv6 SSM group range.	**ssm-policy** *acl-number*	The default range is FF3x::/32, where x means any valid scope.

Configuring common IPv6 PIM features

Configuration task list

Task at a glance
(Optional.) Configuring an IPv6 multicast data filter
(Optional.) Configuring a hello message filter
(Optional.) Configuring IPv6 PIM hello message options
(Optional.) Configuring common IPv6 PIM timers
(Optional.) Setting the maximum size of each join or prune message
(Optional.) Enabling IPv6 PIM to work with BFD

Configuration prerequisites

Before you configure common IPv6 PIM features, complete the following tasks:

- 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-SSM.

Configuring an IPv6 multicast data filter

In either an IPv6 PIM-DM domain or an IPv6 PIM-SM domain, routers can check passing-by IPv6 multicast data and determine whether to continue forwarding the IPv6 multicast data based on the configured filtering rules. You can configure an IPv6 PIM router to act as an IPv6 multicast data filter to help implement traffic control and control the information available to downstream receivers.

A filter can filter not only independent IPv6 multicast data but also IPv6 multicast data encapsulated in register messages. Generally, a filter nearer to the IPv6 multicast source has a better filtering effect.

To configure an IPv6 multicast data filter:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter IPv6 PIM view.	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	N/A
3. Configure an IPv6 multicast data filter:	**source-policy** *acl6-number*	By default, no IPv6 multicast data filter is configured.

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 relationship 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 relationship.

To configure a hello message filter:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure a hello message filter.	**ipv6 pim neighbor-policy** *acl6-number*	By default, no hello message filter exists. If an IPv6 PIM neighbor's hello messages cannot pass the filter, the neighbor is automatically removed when its maximum number of hello attempts is reached.

Configuring IPv6 PIM hello message options

In either an IPv6 PIM-DM domain or an IPv6 PIM-SM domain, hello messages exchanged among routers contain the following configurable options:

- **DR_Priority** (for IPv6 PIM-SM only)—Priority for DR election. The device with the highest priority wins the DR election. You can configure this option for all the routers in a shared-media LAN that directly connects to the IPv6 multicast source or the receivers.
- **Holdtime**—IPv6 PIM neighbor lifetime. If a router receives no hello message from a neighbor when the neighbor lifetime expires, it regards the neighbor failed or unreachable.
- **LAN_Prune_Delay**—Delay of forwarding prune messages on a shared-media LAN. This option consists of LAN delay (namely, prune message delay), override interval, and neighbor tracking support (namely, the capability to disable join message suppression).

  The prune message delay defines the delay time for a router to forward a received prune message to the upstream routers. The override interval defines a time period for a downstream router to override a prune message. If the prune message delay or override interval on different IPv6 PIM routers on a shared-media LAN are different, the largest value takes effect.

  A router does not immediately prune an interface after it receives a prune message from the interface. Instead, it starts a timer (the prune message delay plus the override interval). If interface receives a join message before the override interval expires, the router does not prune the interface. Otherwise, the router prunes the interface when the timer (the prune message delay plus the override interval) expires.

  You can enable the neighbor tracking function (or disable the join message suppression function) on an upstream router to track the states of the downstream nodes that have sent the join message and the joined state holdtime timer has not expired. If you want to enable the neighbor tracking function, you must enable it on all IPv6 PIM routers on a shared-media LAN. Otherwise, the upstream router cannot track join messages from every downstream routers..
- **Generation ID**—A router generates a generation ID for hello messages when an interface is enabled with IPv6 PIM. The generation ID is a random value, but only changes when the status of the router changes. 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 router has changed. In this case, it sends a join message to the upstream router for status update. You can configure an

interface to drop hello messages without the generation ID options to promptly know the status of an upstream router.

You can configure hello message options in IPv6 PIM view or interface view. The configurations made in IPv6 PIM view take effect on all interfaces and the configurations made in interface view take effect only on the current interface. If you configure hello message options in both IPv6 PIM view and interface view, the configuration in interface view always takes precedence.

Configuring hello message options globally

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter IPv6 PIM view.	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	N/A
3. Set the DR priority.	**hello-option dr-priority** *priority*	By default, the DR priority is 1.
4. Set the neighbor lifetime.	**hello-option holdtime** *time*	By default, the neighbor lifetime is 105 seconds.
5. Set the prune message delay.	**hello-option lan-delay** *delay*	By default, the prune message delay is 500 milliseconds.
6. Set the override interval.	**hello-option override-interval** *interval*	By default, the override interval is 2500 milliseconds.
7. Enable the neighbor tracking function.	**hello-option neighbor-tracking**	By default, the neighbor tracking function is disabled.

Configuring hello message options on an interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Set the DR priority.	**ipv6 pim hello-option dr-priority** *priority*	By default, the DR priority is 1.
4. Set the neighbor lifetime.	**ipv6 pim hello-option holdtime** *time*	By default, the neighbor lifetime is 105 seconds.
5. Set the prune delay.	**ipv6 pim hello-option lan-delay** *delay*	By default, the prune delay is 500 milliseconds.
6. Set the override interval.	**ipv6 pim hello-option override-interval** *interval*	By default, the override interval is 2500 milliseconds.
7. Enable the neighbor tracking function.	**ipv6 pim hello-option neighbor-tracking**	By default, the neighbor tracking function is disabled.
8. Enable dropping hello messages without the Generation ID option.	**ipv6 pim require-genid**	By default, an interface accepts hello message without the Generation ID option.

Configuring common IPv6 PIM timers

IPv6 PIM routers periodically send hello messages to discover IPv6 PIM neighbors, and maintain IPv6 PIM neighbor relationship.

After receiving a hello message, an IPv6 PIM router waits for a random time period before sending a hello message. This random time period is smaller than the maximum delay for sending hello messages, and it can avoids collisions that might occur when multiple IPv6 PIM routers send hello messages simultaneously.

An IPv6 PIM router periodically sends join/prune messages to its upstream routers for state update. A join/prune message contains the joined/pruned state timeout value, and an upstream router uses this value to set a timeout timer for the joined state or pruned state of the downstream interfaces.

When a router fails to receive subsequent IPv6 multicast data from the IPv6 multicast source S, the router does not immediately remove 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.

You can configure common IPv6 PIM timers in IPv6 PIM view or interface view. The configurations made in IPv6 PIM view take effect on all interfaces and the configurations made in interface view take effect only on the current interface. If you configure hello message options in both IPv6 PIM view and interface view, the configuration in interface view always takes precedence.

TIP:

For a network without special requirements, HP recommends using the defaults.

Configuring common IPv6 PIM timers globally

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter IPv6 PIM view.	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	N/A
3. Set the interval to send hello messages.	**timer hello** *interval*	By default, the interval to send hello messages is 30 seconds.
4. Set the interval to send join/prune messages.	**timer join-prune** *interval*	By default, the interval to send join/prune messages is 60 seconds.
5. Set the joined/pruned state holdtime timer.	**holdtime join-prune** *time*	By default, the joined/pruned state holdtime timer is 210 seconds.
6. Set the IPv6 multicast source lifetime.	**source-lifetime** *time*	By default, the IPv6 multicast source lifetime is 210 seconds.

Configuring common IPv6 PIM timers on an interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Set the interval to send hello messages.	**ipv6 pim timer hello** *interval*	By default, the interval to send hello messages is 30 seconds.

Step	Command	Remarks
4. Set the maximum delay for sending hello messages.	**ipv6 pim triggered-hello-delay** *delay*	By default, the maximum delay for sending hello messages is 5 seconds.
5. Set the interval to send join/prune messages.	**ipv6 pim timer join-prune** *interval*	By default, the interval to send join/prune messages is 60 seconds.
6. Set the joined/pruned state holdtime timer.	**ipv6 pim holdtime join-prune** *time*	By default, the joined/pruned state holdtime timer is 210 seconds.

Setting the maximum size of each join or prune message

The loss of an oversized join or prune message might result in loss of massive information. You can set a small value for the size of each join or prune message to reduce the impact.

To set the maximum size of each join or prune message:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter IPv6 PIM view.	**ipv6 pim** [**vpn-instance** *vpn-instance-name*]	N/A
3. Set the maximum size of each join or prune message.	**jp-pkt-size** *size*	By default, the maximum size of a join or prune message is 8100 bytes.

Enabling IPv6 PIM to work with BFD

IPv6 PIM uses hello messages to elect a DR for a shared-media network. The elected DR is the only multicast forwarder on the shared-media 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 before other routers detect the link failures and trigger a new DR election. To start a new DR election process immediately after the original DR fails, you can enable IPv6 PIM to work with BFD on a shared-media 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 shared-media network, so that the IPv6 PIM neighbors can fast detect DR failures and start a new DR election process. For more information about BFD, see *High Availability Configuration Guide*.

Before you configure this feature on an interface, be sure to enable IPv6 PIM-DM or IPv6 PIM-SM on the interface.

To enable IPv6 PIM to work with BFD:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Enable IPv6 PIM to work with BFD.	**ipv6 pim bfd enable**	By default, IPv6 PIM is disabled to work with BFD.

Displaying and maintaining IPv6 PIM

Execute **display** commands in any view.

Task	Command
Display BSR information in the IPv6 PIM-SM domain.	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **bsr-info**
Display information about the routes used by IPv6 PIM.	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **claimed-route** [*ipv6-source-address*]
Display C-RP information in the IPv6 PIM-SM domain.	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **c-rp** [**local**]
Display IPv6 PIM information on an interface.	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **interface** [*interface-type interface-number*] [**verbose**]
Display IPv6 PIM neighbor information.	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **neighbor** [*ipv6-neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *
Display IPv6 PIM routing table information.	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **routing-table** [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **flags** *flag-value* | **fsm** | **incoming-interface** *interface-type interface-number* | **mode** *mode-type* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number*] *
Display RP information in the IPv6 PIM-SM domain.	**display ipv6 pim** [**vpn-instance** *vpn-instance-name*] **rp-info** [*ipv6-group-address*]

IPv6 PIM configuration examples

IPv6 PIM-DM configuration example

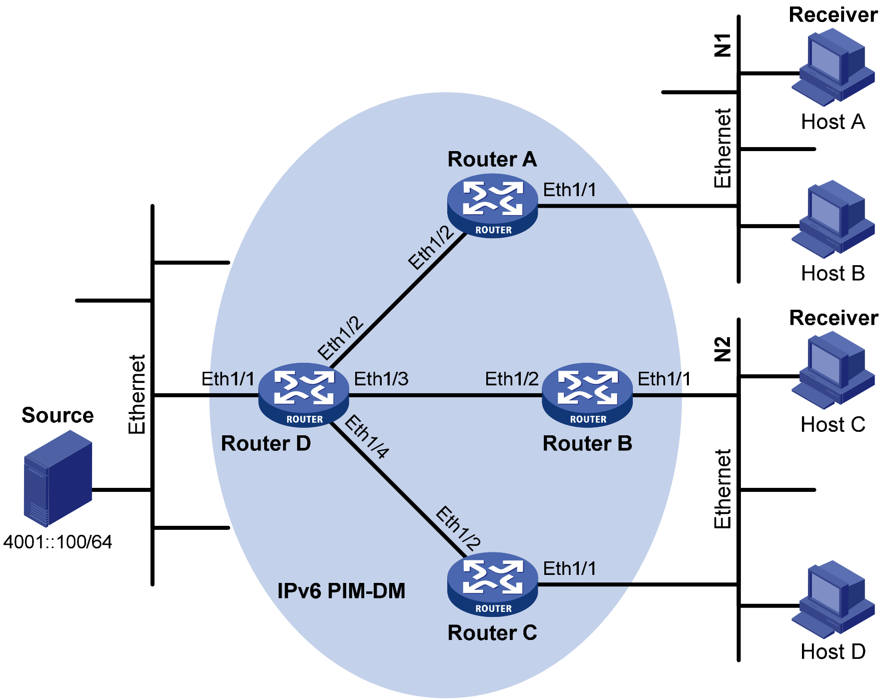
Network requirements

VOD streams are sent to receiver hosts in multicast. The receiver groups of different organizations form stub networks, and at least one receiver host exists in each stub network. The entire IPv6 PIM domain is operating in the dense mode.

Host A and Host C are IPv6 multicast receivers in two stub networks N1 and N2.

MLDv1 runs between Router A and N1 and between Router B, Router C, and N2.

Figure 52 Network diagram



Device	Interface	IPv6 address	Device	Interface	IPv6 address
Router A	Eth1/1	1001::1/64	Router D	Eth1/1	4001::1/64
	Eth1/2	1002::1/64		Eth1/2	1002::2/64
Router B	Eth1/1	2001::1/64		Eth1/3	2002::2/64
	Eth1/2	2002::1/64		Eth1/4	3001::2/64
Router C	Eth1/1	2001::2/64			
	Eth1/2	3001::1/64			

Configuration procedure

1. Assign an IPv6 address and prefix length to each interface according to Figure 52. (Details not shown.)
2. Configure OSPFv3 on the routers in the IPv6 PIM-DM domain to make sure they are interoperable at the network layer and routing information among the routers can be dynamically updated. (Details not shown.)
3. Enable IPv6 multicast routing, MLD, and IPv6 PIM-DM:

   # On Router A, enable IPv6 multicast routing, enable MLD on Ethernet 1/1, and enable IPv6 PIM-DM on each interface.

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] mld enable
[RouterA-Ethernet1/1] ipv6 pim dm
[RouterA-Ethernet1/1] quit
[RouterA] interface ethernet 1/2
[RouterA-Ethernet1/2] ipv6 pim dm
```

```
[RouterA-Ethernet1/2] quit
```

# Enable IPv6 multicast routing, MLD, and IPv6 PIM-DM on Router B and Router C in the same way Router A is configured. (Details not shown.)

# On Router D, enable IPv6 multicast routing and enable IPv6 PIM-DM on each interface.

```
<RouterD> system-view
[RouterD] ipv6 multicast routing
[RouterD-mrib6] quit
[RouterD] interface ethernet 1/1
[RouterD-Ethernet1/1] ipv6 pim dm
[RouterD-Ethernet1/1] quit
[RouterD] interface ethernet 1/2
[RouterD-Ethernet1/2] ipv6 pim dm
[RouterD-Ethernet1/2] quit
[RouterD] interface ethernet 1/3
[RouterD-Ethernet1/3] ipv6 pim dm
[RouterD-Ethernet1/3] quit
[RouterD] interface ethernet 1/4
[RouterD-Ethernet1/4] ipv6 pim dm
[RouterD-Ethernet1/4] quit
```

Verifying the configuration

# Display IPv6 PIM information on Router D.

```
[RouterD] display ipv6 pim interface
 Interface           NbrCnt HelloInt   DR-Pri    DR-Address
 Eth1/1              0      30         1         FE80::A01:201:1
                                                 (local)
 Eth1/2              0      30         1         FE80::A01:201:2
                                                 (local)
 Eth1/3              1      30         1         FE80::A01:201:3
                                                 (local)
 Eth1/4              1      30         1         FE80::A01:201:4
                                                 (local)
```

# Display IPv6 PIM neighboring relationship on Router D.

```
[RouterD] display ipv6 pim neighbor
 Total Number of Neighbors = 3

 Neighbor        Interface           Uptime   Expires  Dr-Priority
 FE80::A01:101:1 Eth1/2              00:04:00 00:01:29 1
 FE80::B01:102:2 Eth1/3              00:04:16 00:01:29 3
 FE80::C01:103:3 Eth1/4              00:03:54 00:01:17 5
```

Assume that Host A needs to receive information addressed to IPv6 multicast group FF0E::101. Once the IPv6 multicast source 4001::100/64 sends IPv6 multicast packets to the IPv6 multicast group, an SPT is established through traffic flooding. Routers on the SPT path (Router A and Router D) have their (S, G) entries. Host A sends an MLD report to Router A to join IPv6 multicast group, and a (*, G) entry is generated on Router A. To display the IPv6 PIM routing information on a router, use the **display ipv6 pim routing-table** command. For example:

# Display IPv6 PIM multicast routing table information on Router A.

```
[RouterA] display ipv6 pim 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: Ethernet1/1
             Protocol: mld, UpTime: 00:01:20, Expires: -

 (4001::100, FF0E::101)
     Protocol: pim-dm, Flag: ACT
     UpTime: 00:01:20
     Upstream interface: Ethernet1/2
         Upstream neighbor: 1002::2
         RPF prime neighbor: 1002::2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Ethernet1/1
             Protocol: pim-dm, UpTime: 00:01:20, Expires: -
```

# Display IPv6 PIM multicast routing table information on Router D.

```
[RouterD] display ipv6 pim 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: Ethernet1/1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 2
         1: Ethernet1/2
             Protocol: pim-dm, UpTime: 00:02:19, Expires: -
         2: Ethernet1/4
             Protocol: pim-dm, UpTime: 00:02:19, Expires: -
```

IPv6 PIM-SM non-scoped zone configuration example

Network requirements

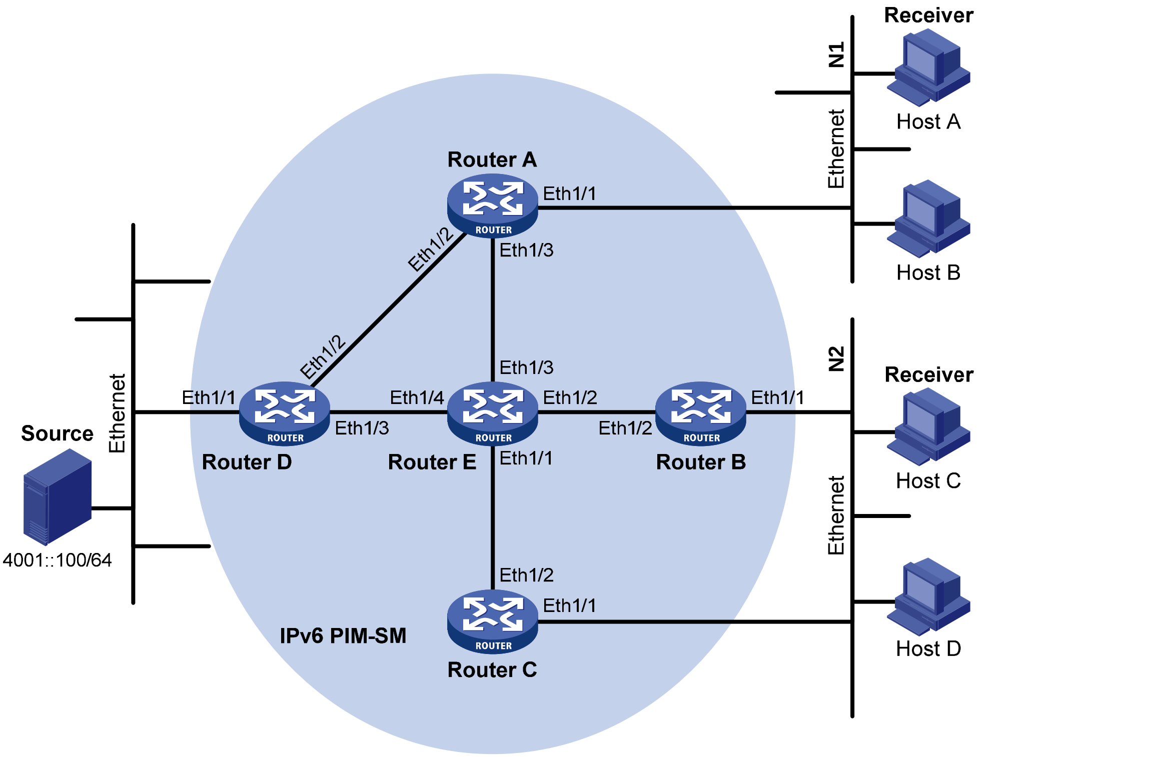
As shown in Figure 53, VOD streams are sent to receiver hosts in multicast. The receivers of different subnets form stub networks, and at least one receiver host exist in each stub network. The entire IPv6 PIM-SM domain contains only one BSR.

Host A and Host C are multicast receivers in the stub networks N1 and N2.

Ethernet1/3 on Router D and Ethernet1/3 on Router E act as C-BSRs and C-RPs. The C-BSR on Router E has a higher priority. The C-RPs are designated to the IPv6 multicast group range FF0E::101/64. Modify the hash mask length to map the IPv6 multicast group range to the two C-RPs.

MLDv1 runs between Router A and N1, and between Router B, Router C, and N2.

Figure 53 Network diagram



Device	Interface	IPv6 address	Device	Interface	IPv6 address
Router A	Eth1/1	1001::1/64	Router D	Eth1/1	4001::1/64
	Eth1/2	1002::1/64		Eth1/2	1002::2/64
	Eth1/3	1003::1/64		Eth1/3	4002::1/64
Router B	Eth1/1	2001::1/64	Router E	Eth1/1	3001::2/64
	Eth1/2	2002::1/64		Eth1/2	2002::2/64
Router C	Eth1/1	2001::2/64		Eth1/3	1003::2/64
	Eth1/2	3001::1/64		Eth1/4	4002::2/64

Configuration procedure

1. Assign an IPv6 address and prefix length to each interface according to Figure 53. (Details not shown.)
2. Enable OSPFv3 on all routers on the IPv6 PIM-SM network to make sure the network-layer on the IPv6 PIM-SM network is interoperable and the routing information among the routers can be dynamically updated. (Details not shown.)
3. Enable IPv6 multicast routing, and enable MLD and IPv6 PIM-SM:

   # On Router A, enable IPv6 multicast routing globally, enable MLD on Ethernet 1/1, and enable IPv6 PIM-SM on each interface.

   ```
   <RouterA> system-view
   ```

```
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] mld enable
[RouterA-Ethernet1/1] ipv6 pim sm
[RouterA-Ethernet1/1] quit
[RouterA] interface ethernet 1/2
[RouterA-Ethernet1/2] ipv6 pim sm
[RouterA-Ethernet1/2] quit
[RouterA] interface ethernet 1/3
[RouterA-Ethernet 1/3] ipv6 pim sm
[RouterA-Ethernet 1/3] quit
```

# Enable IPv6 multicast routing, MLD and IPv6 PIM-SM on Router B and Router C in the same way Router A is configured. (Details not shown.)

# Enable IPv6 multicast routing and IPv6 PIM-SM on Router D and Router E in the same way Router A is configured. (Details not shown.)

4. Configure C-BSRs and C-RPs:

# On Router D, configure the service scope of RP advertisements, configure Ethernet 1/3 as a C-BSR and a C-RP, and set the hash mask length to 128 and the priority of the C-BSR to 10.

```
<RouterD> system-view
[RouterD] acl ipv6 number 2005
[RouterD-acl6-basic-2005] rule permit source ff0e::101 64
[RouterD-acl6-basic-2005] quit
[RouterD] ipv6 pim
[RouterD-pim6] c-bsr 4002::1 hash-length 128 priority 10
[RouterD-pim6] c-rp 4002::1 group-policy 2005
[RouterD-pim6] quit
```

# On Router E, configure the service scope of RP advertisements, configure Ethernet 1/3 as a C-BSR and a C-RP, and set the hash mask length to 128 and the priority of the C-BSR to 20.

```
<RouterE> system-view
[RouterE] acl ipv6 number 2005
[RouterE-acl6-basic-2005] rule permit source ff0e::101 64
[RouterE-acl6-basic-2005] quit
[RouterE] ipv6 pim
[RouterE-pim6] c-bsr 1003::2 hash-length 128 priority 20
[RouterE-pim6] c-rp 1003::2 group-policy 2005
[RouterE-pim6] quit
```

Verifying the configuration

# Display IPv6 PIM information on Router A.

```
[RouterA] display ipv6 pim interface
 Interface           NbrCnt HelloInt   DR-Pri    DR-Address
 Eth1/1              0      30         1         FE80::A01:201:1
                                                 (local)
 Eth1/2              1      30         1         FE80::A01:201:2
 Eth1/2              1      30         1         FE80::A01:201:2
```

# Display BSR information on Router A.

```
[RouterA] display ipv6 pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:46
     Elected BSR address: 1003::2
       Priority: 20
       Hash mask length: 128
       Uptime: 00:04:22
```

# Display BSR information on Router D.

```
[RouterD] display ipv6 pim bsr-info
 Scope: non-scoped
     State: Candidate
     Bootstrap timer: 00:01:45
     Elected BSR address: 1003::2
       Priority: 20
       Hash mask length: 128
       Uptime: 00:05:26
     Candidate BSR address: 4002::1
       Priority: 10
       Hash mask length: 128
```

# Display BSR information on Router E.

```
[RouterE] display ipv6 pim bsr-info
 Scope: non-scoped
     State: Elected
     Bootstrap timer: 00:01:48
     Elected BSR address: 1003::2
       Priority: 20
       Hash mask length: 128
       Uptime: 00:01:10
     Candidate BSR address: 1003::2
       Priority: 20
       Hash mask length: 128
```

# Display RP information on Router A.

```
[RouterA] display ipv6 pim rp-info
   BSR RP information:
 Scope: non-scoped
     Group/MaskLen: FF0E::101/64
       RP address               Priority  HoldTime  Uptime    Expires
       1003::2                  192       180       00:05:19  00:02:11
       4002::1                  192       180       00:05:19  00:02:11
```

IPv6 PIM-SM admin-scoped zone configuration example

Network requirements

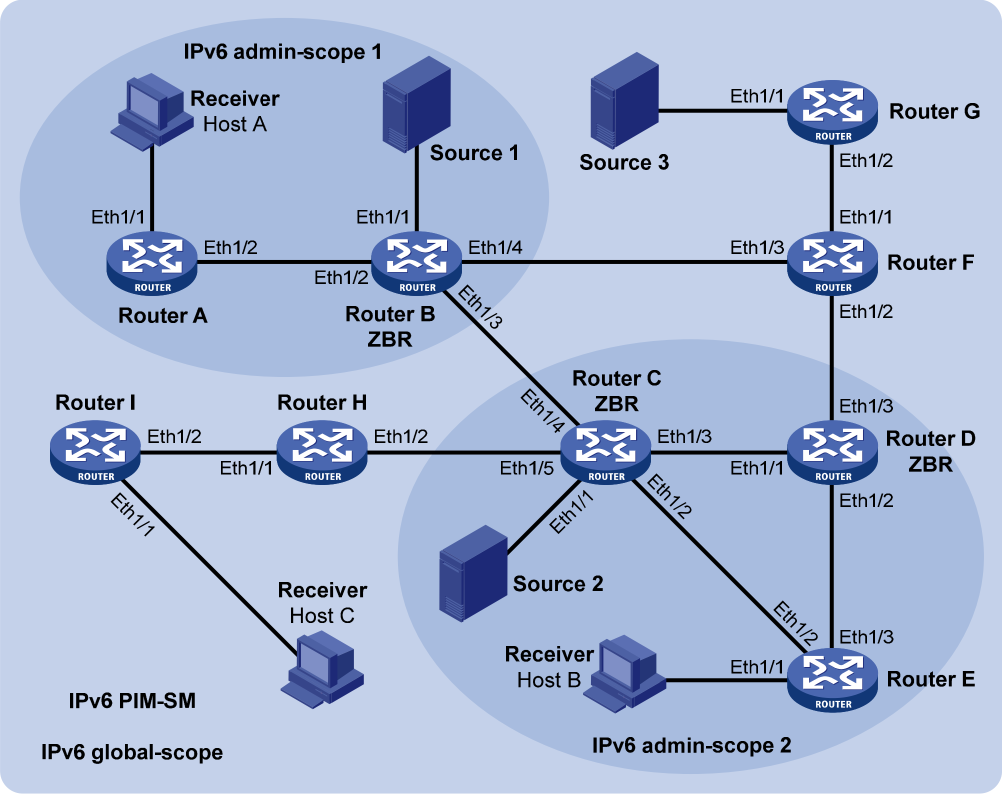
As shown in Figure 54, VOD streams are sent to receiver hosts in multicast. The entire IPv6 PIM-SM domain is divided into IPv6 admin-scoped zone 1, IPv6 admin-scoped zone 2, and the IPv6 global-scoped zone. Router B, Router C, and Router D are ZBRs of the three zones, respectively.

Source 1 and Source 2 send different IPv6 multicast data to the IPv6 multicast group FF14::101. Host A receives the IPv6 multicast data only from Source 1, and Host B receives the IPv6 multicast data only from Source 2. Source 3 sends IPv6 multicast data to the IPv6 multicast group FF1E::202. Host C is an IPv6 multicast receiver for the IPv6 multicast group FF1E::202.

Ethernet 1/2 of Router B acts as a C-BSR and a C-RP for IPv6 admin-scoped zone 1, and Ethernet 1/1 of Router D acts as a C-BSR and a C-RP for IPv6 admin-scoped zone 2. Both of the two interfaces are designated to the IPv6 multicast groups with the scope field of 4. Ethernet 1/1 of Router F acts as a C-BSR and a C-RP for the IPv6 global-scoped zone, and is designated to the IPv6 multicast groups with the scope field value of 14.

MLDv1 separately runs between Router A, Router E, Router I, and the receivers that directly connect to them.

Figure 54 Network diagram



Device	Interface	IPv6 address	Device	Interface	IPv6 address
Router A	Eth1/1	1001::1/64	Router D	Eth1/1	3003::2/64
	Eth1/2	1002::1/64		Eth1/3	6001::1/64
Router B	Eth1/1	2001::1/64		Eth1/3	6002::1/64
	Eth1/2	1002::2/64	Router E	Eth1/1	7001::1/64
	Eth1/3	2002::1/64		Eth1/2	3002::2/64
	Eth1/4	2003::1/64		Eth1/3	6001::2/64
Router C	Eth1/1	3001::1/64	Router F	Eth1/1	8001::1/64
	Eth1/2	3002::1/64		Eth1/2	6002::2/64
	Eth1/3	3003::1/64		Eth1/3	2003::2/64
	Eth1/4	2002::2/64	Router G	Eth1/1	9001::1/64
	Eth1/5	3004::1/64		Eth1/2	8001::2/64

Device	Interface	IPv6 address	Device	Interface	IPv6 address
Router H	Eth1/1	4001::1/64	Source 1	-	2001::100/64
	Eth1/2	3004::2/64	Source 2	-	3001::100/64
Router I	Eth1/1	5001::1/64	Source 3	-	9001::100/64
	Eth1/2	4001::2/64			

Configuration procedure

1. Assign an IPv6 address and prefix length to each interface according to Figure 54. (Details not shown.)
2. Enable OSPFv3 on all routers on the IPv6 PIM-SM network to make sure the network-layer on the IPv6 PIM-SM network is interoperable and the routing information among the routers can be dynamically updated. (Details not shown.)
3. Enable IPv6 multicast routing, MLD, and IPv6 PIM-SM:

   # On Router A, enable IPv6 multicast routing globally, enable MLD on Ethernet 1/1, and enable IPv6 PIM-SM on each interface.

   ```
   <RouterA> system-view
   [RouterA] ipv6 multicast routing
   [RouterA-mrib6] quit
   [RouterA] interface ethernet 1/1
   [RouterA-Ethernet1/1] mld enable
   [RouterA-Ethernet1/1] ipv6 pim sm
   [RouterA-Ethernet1/1] quit
   [RouterA] interface ethernet 1/2
   [RouterA-Ethernet1/2] ipv6 pim sm
   [RouterA-Ethernet1/2] quit
   ```

   # Enable IPv6 multicast routing, MLD, and IPv6 PIM-SM on Router E and Router I in the same way Router A is configured. (Details not shown.)

   # On Router B, enable IPv6 multicast routing globally, and enable IPv6 PIM-SM on each interface.

   ```
   <RouterB> system-view
   [RouterB] ipv6 multicast routing
   [RouterB-mrib6] quit
   [RouterB] interface ethernet 1/1
   [RouterB-Ethernet1/1] ipv6 pim sm
   [RouterB-Ethernet1/1] quit
   [RouterB] interface ethernet 1/2
   [RouterB-Ethernet1/2] ipv6 pim sm
   [RouterB-Ethernet1/2] quit
   [RouterB] interface ethernet 1/3
   [RouterB-Ethernet1/3] ipv6 pim sm
   [RouterB-Ethernet1/3] quit
   [RouterB] interface ethernet 1/4
   [RouterB-Ethernet1/4] ipv6 pim sm
   [RouterB-Ethernet1/4] quit
   ```

   # Enable IPv6 multicast routing and IPv6 PIM-SM on Router C, Router D, Router F, Router G, and Router H in the same way Router B is configured. (Details not shown.)
4. Configure IPv6 admin-scoped zone boundaries:

# On Router B, configure Ethernet 1/3 and Ethernet 1/4 as the boundaries of IPv6 admin-scoped zone 1.

```
[RouterB] interface ethernet 1/3
[RouterB-Ethernet1/3] ipv6 multicast boundary scope 4
[RouterB-Ethernet1/3] quit
[RouterB] interface ethernet 1/4
[RouterB-Ethernet1/4] ipv6 multicast boundary scope 4
[RouterB-Ethernet1/4] quit
```

# On Router C, configure Ethernet 1/4 and Ethernet 1/5 as the boundaries of IPv6 admin-scoped zone 2.

```
<RouterC> system-view
[RouterC] interface ethernet 1/4
[RouterC-Ethernet1/4] ipv6 multicast boundary scope 4
[RouterC-Ethernet1/4] quit
[RouterC] interface ethernet 1/5
[RouterC-Ethernet1/5] ipv6 multicast boundary scope 4
[RouterC-Ethernet1/5] quit
```

# On Router D, configure Ethernet 1/3 as the boundary of IPv6 admin-scoped zone 2.

```
<RouterD> system-view
[RouterD] interface ethernet 1/3
[RouterD-Ethernet1/3] ipv6 multicast boundary scope 4
[RouterD-Ethernet1/3] quit
```

5. Configure C-BSRs and C-RPs:

   # On Router B, configure the service scope of RP advertisements and configure Ethernet 1/2 as a C-BSR and a C-RP for IPv6 admin-scoped zone 1.

```
[RouterB] ipv6 pim
[RouterB-pim6] c-bsr 1002::2 scope 4
[RouterB-pim6] c-rp 1002::2 scope 4
[RouterB-pim6] quit
```

   # On Router D, configure the service scope of RP advertisements and configure Ethernet 1/1 as a C-BSR and a C-RP for IPv6 admin-scoped zone 2.

```
[RouterD] ipv6 pim
[RouterD-pim6] c-bsr 3003::2 scope 4
[RouterD-pim6] c-rp 3003::2 scope 4
[RouterD-pim6] quit
```

   # On Router F, configure Ethernet 1/1 as a C-BSR and a C-RP for the IPv6 global-scoped zone.

```
<RouterF> system-view
[RouterF] ipv6 pim
[RouterF-pim6] c-bsr 8001::1
[RouterF-pim6] c-rp 8001::1
[RouterF-pim6] quit
```

Verifying the configuration

# Display BSR information on Router B.

```
[RouterB] display ipv6 pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:25
     Elected BSR address: 8001::1
       Priority: 64
       Hash mask length: 126
       Uptime: 00:01:45

 Scope: 4
     State: Elected
     Bootstrap timer: 00:00:06
     Elected BSR address: 1002::2
       Priority: 64
       Hash mask length: 126
       Uptime: 00:04:54
     Candidate BSR address: 1002::2
       Priority: 64
       Hash mask length: 126
```

# Display BSR information on Router D.

```
[RouterD] display ipv6 pim bsr-info
 Scope: non-scoped
     State: Accept Preferred
     Bootstrap timer: 00:01:25
     Elected BSR address: 8001::1
       Priority: 64
       Hash mask length: 126
       Uptime: 00:01:45

   Scope: 4
     State: Elected
     Bootstrap timer: 00:01:25
     Elected BSR address: 3003::2
       Priority: 64
       Hash mask length: 126
       Uptime: 00:01:45
     Candidate BSR address: 3003::2
       Priority: 64
       Hash mask length: 126
```

# Display BSR information on Router F.

```
[RouterF] display ipv6 pim bsr-info
 Scope: non-scoped
     State: Elected
     Bootstrap timer: 00:00:49
     Elected BSR address: 8001::1
       Priority: 64
       Hash mask length: 126
       Uptime: 00:01:11
     Candidate BSR address: 8001::1
       Priority: 64
       Hash mask length: 126
```

Display RP information on Router B.

```
[RouterB] display ipv6 pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: FF00::/8
       RP address               Priority  HoldTime  Uptime    Expires
       8001::1                  192       180       00:01:14  00:02:46
 Scope: 4
     Group/MaskLen: FF04::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF14::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF24::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF34::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF44::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF54::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF64::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF74::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF84::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF94::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FFA4::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FFB4::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FFC4::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FFD4::/16
```

```
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FFE4::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FFF4::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
     Group/MaskLen: FF04::/16
       RP address               Priority  HoldTime  Uptime    Expires
       1002::2 (local)          192       180       00:02:03  00:02:56
```

# Display RP information on Router F.

```
[RouterF] display pim rp-info
 BSR RP information:
   Scope: non-scoped
     Group/MaskLen: FF00::/8
       RP address               Priority  HoldTime  Uptime    Expires
       8001::1 (local)          192       180       00:10:28  00:02:31
```

IPv6 PIM-SSM configuration example

Network requirements

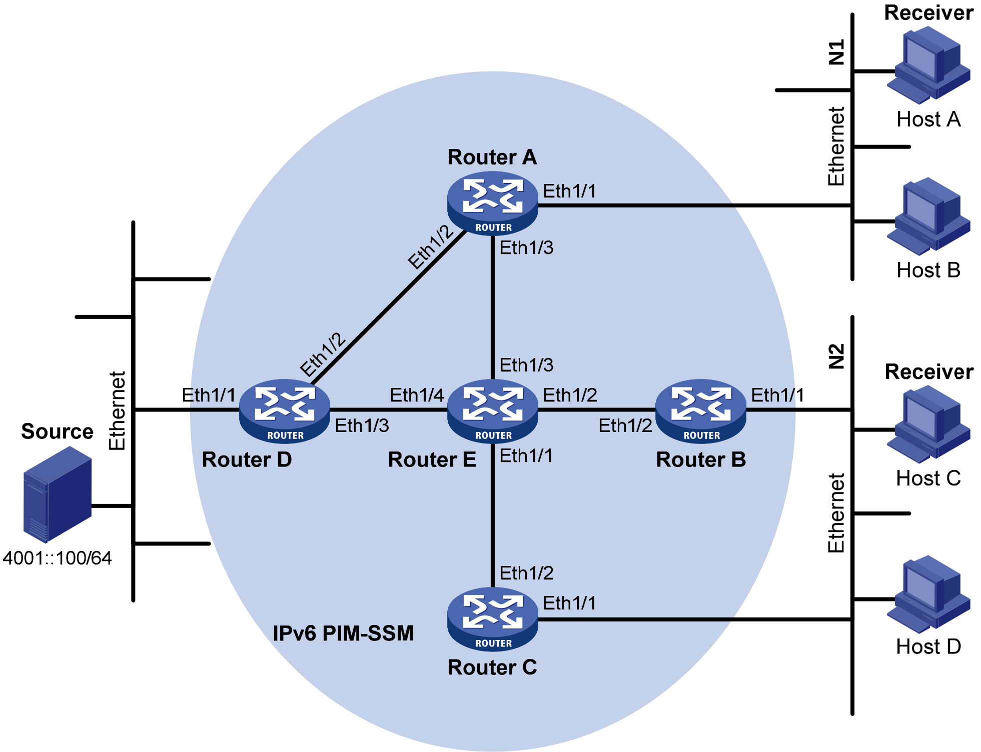
The receivers receive VOD information through multicast. The receiver groups of different organizations form stub networks, and one or more receiver hosts exist in each stub network. The entire IPv6 PIM domain operates in the SSM mode.

Host A and Host C are IPv6 multicast receivers in two stub networks, N1 and N2.

The SSM group range is FF3E::/64.

MLDv2 runs between Router A and N1 and between Router B, Router C, and N2.

Figure 55 Network diagram



Device	Interface	IPv6 address	Device	Interface	IPv6 address
Router A	Eth1/1	1001::1/64	Router D	Eth1/1	4001::1/64
	Eth1/2	1002::1/64		Eth1/2	1002::2/64
	Eth1/3	1003::1/64		Eth1/3	4002::1/64
Router B	Eth1/1	2001::1/64	Router E	Eth1/1	3001::2/64
	Eth1/2	2002::1/64		Eth1/2	2002::2/64
Router C	Eth1/1	2001::2/64		Eth1/3	1003::2/64
	Eth1/2	3001::1/64		Eth1/4	4002::2/64

Configuration procedure

1. Enable IPv6 forwarding on each router and configure the IPv6 address and prefix length for each interface according to Figure 55. (Details not shown.)
2. Configure OSPFv3 on the routers in the IPv6 PIM-SSM domain to make sure they are interoperable at the network layer. (Details not shown.)
3. Enable IPv6 multicast routing, MLD and IPv6 PIM-SM:

   # On Router A, enable IPv6 multicast routing globally, enable MLDv2 on Ethernet 1/1, and enable IPv6 PIM-SM on each interface.

```
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
[RouterA] interface ethernet 1/1
[RouterA-Ethernet1/1] mld enable
[RouterA-Ethernet1/1] mld version 2
[RouterA-Ethernet1/1] ipv6 pim sm
[RouterA-Ethernet1/1] quit
```

```
[RouterA] interface ethernet 1/2
[RouterA-Ethernet1/2] ipv6 pim sm
[RouterA-Ethernet1/2] quit
[RouterA] interface ethernet 1/3
[RouterA-Ethernet1/3] ipv6 pim sm
[RouterA-Ethernet1/3] quit
```

# Enable IPv6 multicast routing, MLD and IPv6 PIM-SM on Router B and Router C in the same way Router A is configured. (Details not shown.)

# Enable IPv6 multicast routing and IPv6 PIM-SM on Router D and Router E in the same way Router A is configured. (Details not shown.)

4. Configure the IPv6 SSM group range to be FF3E::/64 on Router A.

```
[RouterA] acl ipv6 number 2000
[RouterA-acl6-basic-2000] rule permit source ff3e:: 64
[RouterA-acl6-basic-2000] quit
[RouterA] ipv6 pim
[RouterA-pim6] ssm-policy 2000
[RouterA-pim6] quit
```

5. Configure the IPv6 SSM group range on Router B, Router C, Router D and Router E in the same way Router A is configured. (Details not shown.)

Verifying the configuration

# Display IPv6 PIM information on Router A.

```
[RouterA] display ipv6 pim interface
 Interface              NbrCnt HelloInt   DR-Pri   DR-Address
 Eth1/1                 0      30         1        1001::1
                                                   (local)
 Eth1/2                 1      30         1        1002::2
 Eth1/3                 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 multicast group G (FF3E::101). Router A builds an SPT toward the multicast source. Routers on the SPT path (Router A and Router D) have generated an (S, G) entry, but Router E, which is not on the SPT path, does not have multicast routing entries. You can use the **display ipv6 pim routing-table** command to display PIM routing table information on each router. For example:

# Display IPv6 PIM multicast routing table information on Router A.

```
[RouterA] display ipv6 pim routing-table
 Total 0 (*, G) entry; 1 (S, G) entry

 (4001::100, FF3E::101)
     Protocol: pim-ssm, Flag:
     UpTime: 00:00:11
     Upstream interface: Ethernet1/2
         Upstream neighbor: 1002::2
         RPF prime neighbor: 1002::2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Ethernet1/1
             Protocol: mld, UpTime: 00:00:11, Expires: 00:03:25
```

# Display IPv6 PIM multicast routing table information on Router D.

```
[RouterD] display ipv6 pim 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: Ethernet1/1
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Ethernet1/2
             Protocol: pim-ssm, UpTime: 00:08:02, Expires: 00:03:25
```

Troubleshooting IPv6 PIM

A multicast distribution tree cannot be correctly built

Symptom

An IPv6 multicast distribution tree cannot be correctly built because there are no IPv6 multicast forwarding entries established on the routers (including routers directly connected with multicast sources or receivers) in a IPv6 PIM network.

Analysis

- On an IPv6 PIM-DM enabled network, IPv6 multicast data is flooded from the router that directly connects to the IPv6 multicast source to the routers that directly connects to the receivers. When the IPv6 multicast data is flooded to a router, the router creates an (S, G) entry only if it has a route to the IPv6 multicast source. If the router does not have a route to the IPv6 multicast source, or if IPv6 PIM-DM is not enabled on the RPF interface toward the IPv6 multicast source, the router cannot create an (S, G) entry.
- On an IPv6 PIM-SM enabled network, when a router wants to join the SPT, the router creates an (S, G) entry only if it has a route to the IPv6 multicast source. If the router does not have a route to the IPv6 multicast source, or if IPv6 PIM-SM is not enabled on the RPF interface toward the IPv6 multicast source, the router cannot create an (S, G) entry.
- When a multicast router receives an IPv6 multicast packet, it looks up the existing IPv6 unicast routing table for the optimal route to the packet source. The outgoing interface of this route act as the RPF interface and the next hop acts the RPF neighbor. The RPF interface completely relies on the existing IPv6 unicast route and is independent of IPv6 PIM. The RPF interface must be enabled with IPv6 PIM, and the RPF neighbor must be an IPv6 PIM neighbor. If IPv6 PIM is not enabled on the RPF interface or the RPF neighbor, the multicast distribution tree cannot be correctly built, causing abnormal multicast forwarding.
- Because a hello message does not carry IPv6 PIM mode information, an IPv6 PIM router cannot identify what IPv6 PIM mode its IPv6 PIM neighbor is running in. If the RPF interface on a router and the connected interface of the router's RPF neighbor operate in different IPv6 PIM modes, the multicast distribution tree cannot be correctly built, causing abnormal multicast forwarding.

- The same IPv6 PIM mode must run on the entire network. Otherwise, the multicast distribution tree cannot be correctly built, causing abnormal multicast forwarding.

Solution

1. Use **display ipv6 routing-table** to verify that an IPv6 unicast route to the IPv6 multicast source or the RP is available.
2. Use **display ipv6 pim interface** to verify IPv6 PIM information on each interface, especially on the RPF interface. If IPv6 PIM is not enabled on the interfaces, use **ipv6 pim dm** or **ipv6 pim sm** to enable IPv6 PIM-DM or IPv6 PIM-SM for the interfaces.
3. Use **display ipv6 pim neighbor** to verify that the RPF neighbor is an IPv6 PIM neighbor.
4. Verify that IPv6 PIM and MLD are enabled on the interfaces that directly connect to the IPv6 multicast sources or the receivers.
5. Use **display ipv6 pim interface verbose** to verify that the same IPv6 PIM mode is enabled on the RPF interface on a router and the connected interface of the router's RPF neighbor.
6. Use **display current-configuration** to verify that the same IPv6 PIM mode is enabled on all routers on the network. For IPv6 PIM-SM, verify that the BSR and C-RPs are correctly configured.

IPv6 multicast data is 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 IPv6 multicast data but does not create an (S, G) entry in the IPv6 PIM routing table.

Analysis

- If an IPv6 multicast forwarding boundary has been configured through the **ipv6 multicast boundary** command, and the IPv6 multicast packets are kept from crossing the boundary, IPv6 PIM cannot create routing entries for the packets.
- If an ACL is defined by the **source-policy** command, and the IPv6 multicast packets cannot match the ACL rules, IPv6 PIM cannot create the routing entries for the packets.

Solution

1. Use **display current-configuration** to verify the IPv6 multicast forwarding boundary settings. Use **ipv6 multicast boundary** to change the multicast forwarding boundary settings to make the IPv6 multicast packet able to cross the boundary.
2. Use **display current-configuration** to verify the IPv6 multicast data filter. Change the ACL rule defined in the **source-policy** command so that the source/group address of the IPv6 multicast data can pass ACL filtering.

An RP cannot join an SPT in IPv6 PIM-SM

Symptom

An RPT cannot be correctly built, or an RP cannot join the SPT toward the IPv6 multicast source.

Analysis

- RPs are the core of an IPv6 PIM-SM domain. An RP provides services for a specific IPv6 multicast group, and multiple RPs can coexist on a network. Make sure the RP information on all routers is exactly the same to map a specific IPv6 multicast group to the same RP. Otherwise, IPv6 multicast forwarding fails.
- If a static RP is configured, use the same static RP configuration on all routers on the entire network. Otherwise, IPv6 multicast forwarding fails.

Solution

1. Use **display ipv6 routing-table** to verify that an IPv6 unicast route to the RP is available on each router.
2. Use **display ipv6 pim rp-info** to verify that the dynamic RP information is consistent on all routers.
3. Use **display ipv6 pim rp-info** to verify that the same static RPs are configured on all routers on the network.

An RPT cannot be built or IPv6 multicast source registration fails in IPv6 PIM-SM

Symptom

The C-RPs cannot unicast advertisement messages to the BSR. The BSR does not advertise BSMs containing C-RP information and has no IPv6 unicast route to any C-RP. An RPT cannot be correctly established, or the source-side DR cannot register the IPv6 multicast source with the RP.

Analysis

- The C-RPs periodically send advertisement messages to the BSR by unicast. If a C-RP has no IPv6 unicast route to the BSR, it cannot send advertisement messages to the BSR, and the BSR cannot advertise BSMs containing the information of the C-RP.
- If the BSR does not have an IPv6 unicast route to a C-RP, it discards the advertisement messages from the C-RP. Therefore, the BSR cannot advertise BSMs containing the information of the C-RP.
- RPs are the core of an IPv6 PIM-SM domain. Make sure the RP information on all routers is exactly the same to map a specific IPv6 multicast group to the same RP, and that an IPv6 unicast route to the RP are available on the routers.

Solution

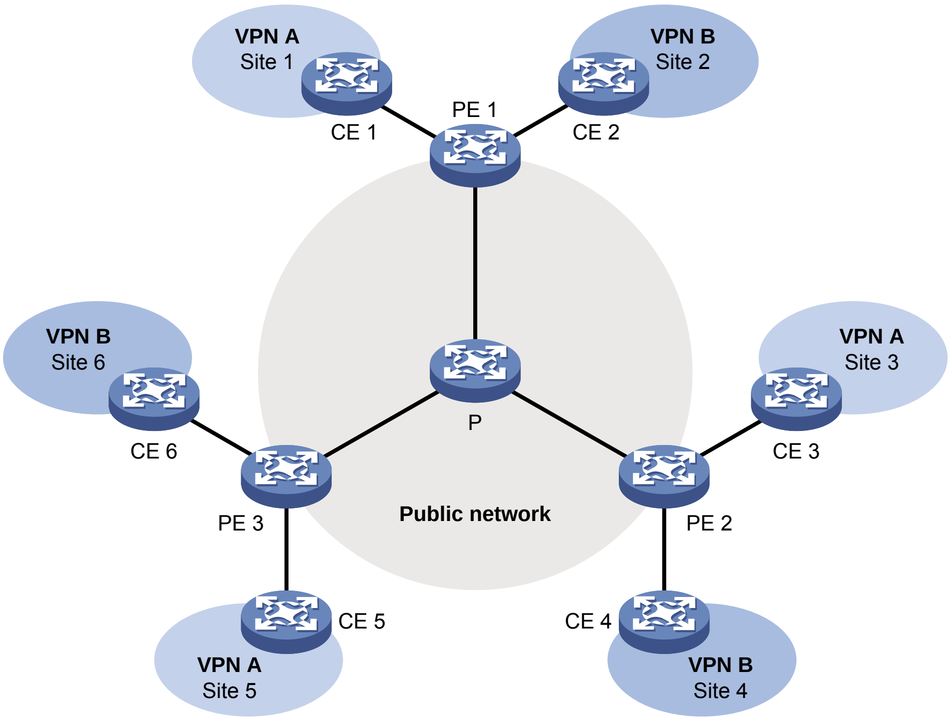
1. Use **display ipv6 routing-table** to verify that the IPv6 unicast routes to the C-RPs and the BSR are available on each router and that a route is available between each C-RP and the BSR. Make sure each C-RP has an IPv6 unicast route to the BSR, the BSR has an IPv6 unicast route to each C-RP, and each router on the network has IPv6 unicast routes to the C-RPs.
2. Use **display ipv6 pim bsr-info** to verify that the BSR information exists on each router, and then use **display ipv6 pim rp-info** to verify that the RP information is correct on each router.
3. Use **display ipv6 pim neighbor** to verify that IPv6 PIM neighboring relationship has been correctly established among the routers.

Configuring multicast VPN

Overview

Multicast VPN is a technique that implements multicast delivery in VPNs. A VPN comprises multiple sites of the customer network and the public network provided by the network service provider. The sites communicate through the public network. As shown in Figure 56, VPN A comprises Site 1, Site 3, and Site 5, and VPN B comprises Site 2, Site 4, and Site 6.

Figure 56 Typical VPN networking diagram

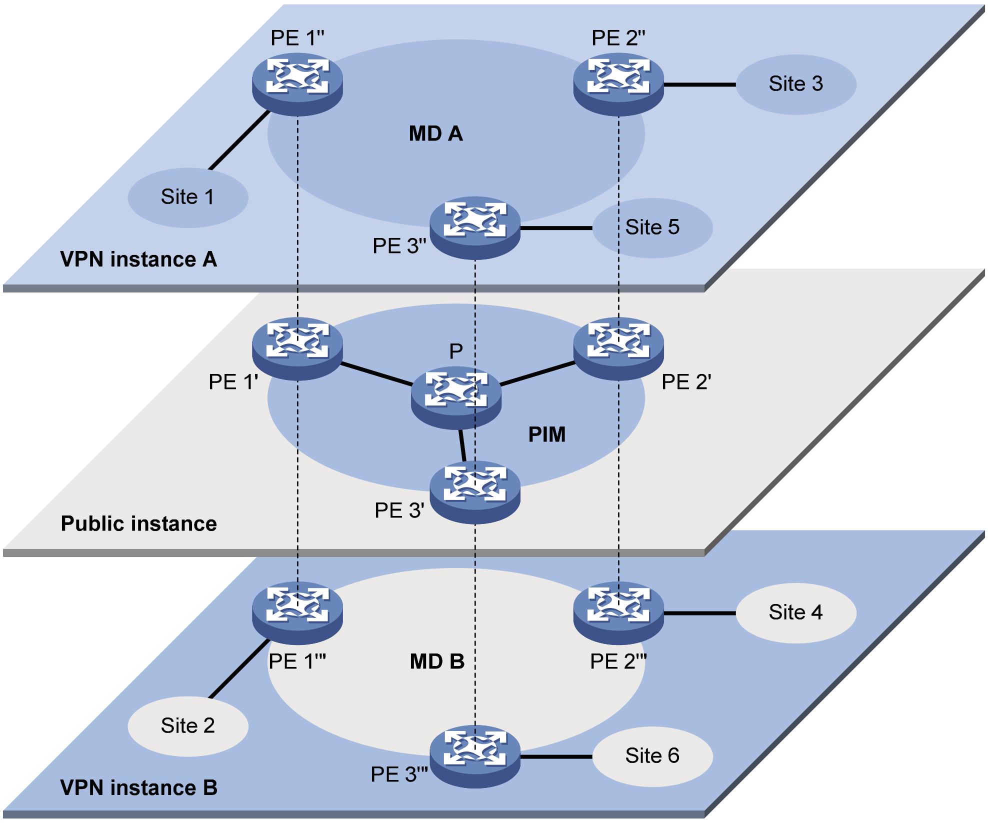


A VPN includes the following types of devices:

- **Provider (P) device**—Core device on the public network. A P device does not directly connect to CE devices.
- **Provider edge (PE) device**—Edge device on the public network. A PE device directly connects to one or more customer edge (CE) devices and processes VPN routing.
- **CE device**—Edge device on a customer network to implement route distribution on the customer network. A CE device can be a router, a switch, or a host.

As shown in Figure 56, the network that runs multicast VPN provides independent multicast services for the public network, VPN A, and VPN B. The multicast device PE supports multiple VPN instances and acts as multiple independent multicast devices. Each VPN forms a plane, and all these planes are isolated from each other. For example, in Figure 56, PE 1 supports the public network, VPN A, and VPN B. You can regard these instances on PE 1 as independent virtual devices, which are PE 1', PE 1", and PE 1'". Each virtual device works on a plane as shown in Figure 57.

Figure 57 Multicast in multiple VPN instances



Through multicast VPN, when a multicast source in VPN A sends a multicast stream to a multicast group, only the multicast group receivers in Site 1, Site 3, and Site 5 of VPN A can receive the multicast stream. The stream is multicast in these sites and on the public network.

The prerequisites for implementing multicast VPN are as follows:

1. Within each site, multicast for a single VPN instance is supported.
2. On the public network, multicast for the public network is supported.
3. The PE devices support multiple VPN instances as follows:
   - Connecting with different sites through VPN instances and supporting multicast for each VPN instance.
   - Connecting with the public network and supporting multicast for the public network.
   - Supporting information exchange and data conversion between the public network and VPNs.

The device implements multicast VPN by using 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 VPN instances. The MD-VPN solution is transparent to CE devices and P devices because multicast VPN can be implemented without the need of upgrading CE devices and P devices or changing their original PIM configurations.

MD-VPN overview

The basic MD-VPN concepts are described in Table 7.

Table 7 Basic MD-VPN concepts

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 constructed by all PE devices in the same VPN.
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 MT. An MTI handles only multicast packets but not unicast packets. The MTI interfaces are automatically created when the MD for the VPN instance is created.
Default-group	On the public network, each MD is assigned a unique multicast address, called a default-group. A default-group is the unique identifier of an MD on the public network. It helps build the default-MDT for an MD on the public network. Each VPN instance is assigned a unique default-group address.
Default-multicast distribution tree (Default-MDT)	A default-MDT uses a default-group address as its group address. In a VPN, the default-MDT is uniquely identified by the default-group. A default-MDT is automatically created after the default-group is specified and will always exist on the public network, regardless of the presence of any multicast services on the public network or the VPN.

Introduction to MD-VPN

The main points in MD-VPN implementation are as follows:

- 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, but the public network multicast traffic between the PE devices and the P devices is transmitted through the public network.
- An MD logically defines the transmission boundary of the multicast traffic of a specific VPN over the public network and physically identifies all the PE devices that support that VPN instance on the public network. Different VPN instances correspond to different MDs.

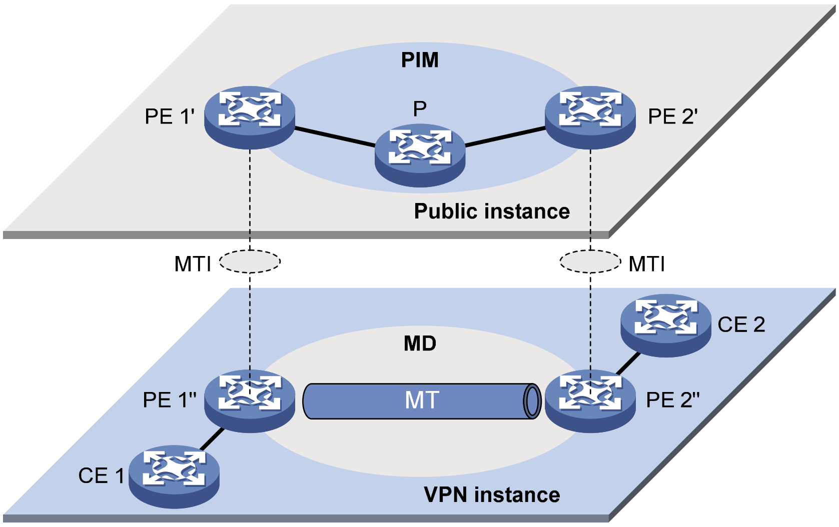
  As shown in Figure 57, the ellipse area in the center of each VPN instance plane represents an MD that provides services for a particular VPN instance. All the VPN multicast traffic in that VPN is transmitted within that MD.
- Inside an MD, all the private traffic is transmitted through the MT. The process of multicast traffic transmission through an MT is as follows:
  a. The local PE device encapsulates a VPN multicast packet into a public network multicast packet.
  b. The encapsulated multicast packet is sent by the PE device and travels over the public network.

c. After receiving the multicast packet, the remote PE device decapsulates the multicast packet to get the original VPN multicast packet.

- The local PE device sends VPN data out of the MTI, and the remote PE devices receive the private data from their MTI interfaces.

  As shown in Figure 58, you can think of an MD as a private data transmission pool and an MTI as an entrance or exit of the pool. The local PE device puts the private data into the transmission pool (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 a remote PE device that needs the data can get it from its exit (MTI).

Figure 58 Relationship between PIM on the public network and an MD in a VPN instance



- Each VPN instance is assigned a unique default-group address. The VPN data is transparent to the public network.

  A PE device encapsulates a VPN multicast packet (a multicast protocol packet or a multicast data packet) into a public network multicast packet, specifying the default-group address as the public network multicast group. Then, the PE sends this multicast packet to the public network.

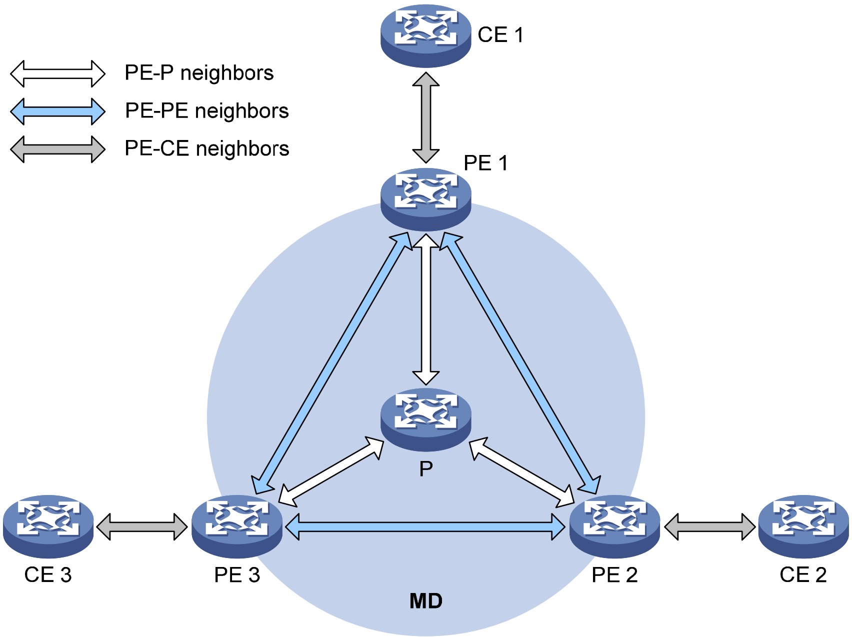
- A default-group corresponds to a unique MD. For each default-group, a unique default-MDT is constructed through the public network resources for multicast data forwarding. All the VPN multicast packets transmitted in this VPN are forwarded along this default-MDT, no matter through which PE device they entered the public network.

NOTE:

A VPN uniquely corresponds to an MD and an MD provides services for only one VPN, which is called a one-to-one relationship. Such a relationship exists between VPN, MD, MTI, and default-group.

PIM neighboring relationships in MD-VPN

Figure 59 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 59, the following types of PIM neighboring relationships exist in MD-VPN:

- **PE-P PIM neighboring relationship**—Established between the public network interface on a PE device and the peer interface on the P device over the link.
- **PE-PE PIM neighboring relationship**—Established between PE devices that are in the same VPN instance after they receive the PIM hello packets.
- **PE-CE PIM neighboring relationship**—Established between a PE interface that is bound with the VPN instance and the peer interface on the CE device over the link.

Protocols and standards

RFC 6037, *Cisco Systems' Solution for Multicast in BGP/MPLS IP VPNs*

How MD-VPN works

This section describes how the MD-VPN technology is implemented, including the default-MDT construction, multicast traffic delivery based on the default-MDT, and inter-AS MD-VPN implementation.

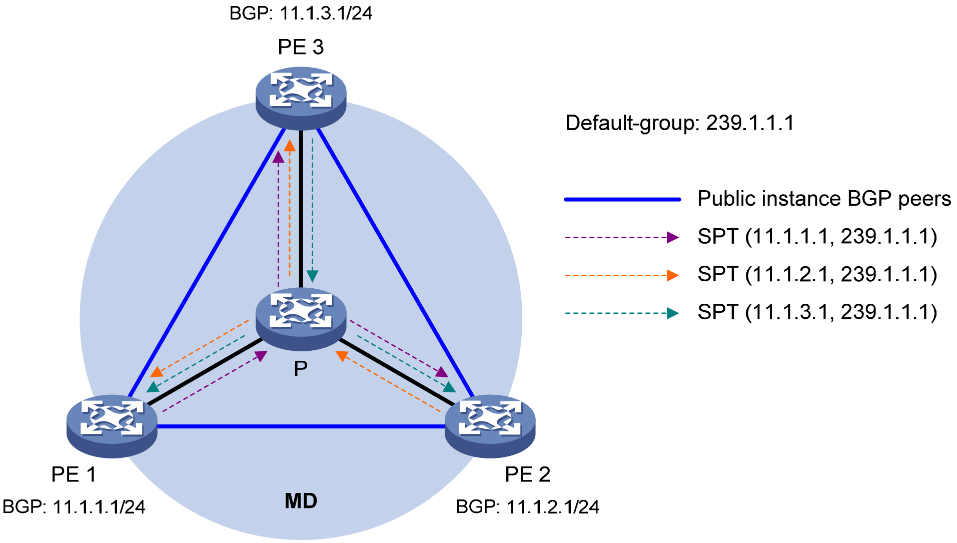
The VPN multicast data transmission on the public network is transparent to this VPN instance. The MTIs at the local PE device and the remote PE device form a channel for the seamless transmission of VPN data over the public network. All that is known to the VPN instance is that the VPN data is sent out of the MTI and then the remote site can receive the data through the MTI. Actually, the multicast data transmission over the public network, or transmission over MDT, is very complicated.

Default-MDT establishment

The multicast routing protocol running on the public network can be PIM-DM or PIM-SM. The process of creating a default-MDT is different in these PIM modes.

Default-MDT establishment in a PIM-DM network

Figure 60 Default-MDT establishment in a PIM-DM network


BGP: 11.1.3.1/24
PE 3
Default-group: 239.1.1.1
Public instance BGP peers
SPT (11.1.1.1, 239.1.1.1)
SPT (11.1.2.1, 239.1.1.1)
SPT (11.1.3.1, 239.1.1.1)
P
PE 1
BGP: 11.1.1.1/24
MD
PE 2
BGP: 11.1.2.1/24

As shown in Figure 60, PIM-DM is enabled in the network and all the PE devices support VPN instance A. The process of establishing a default-MDT is as follows:

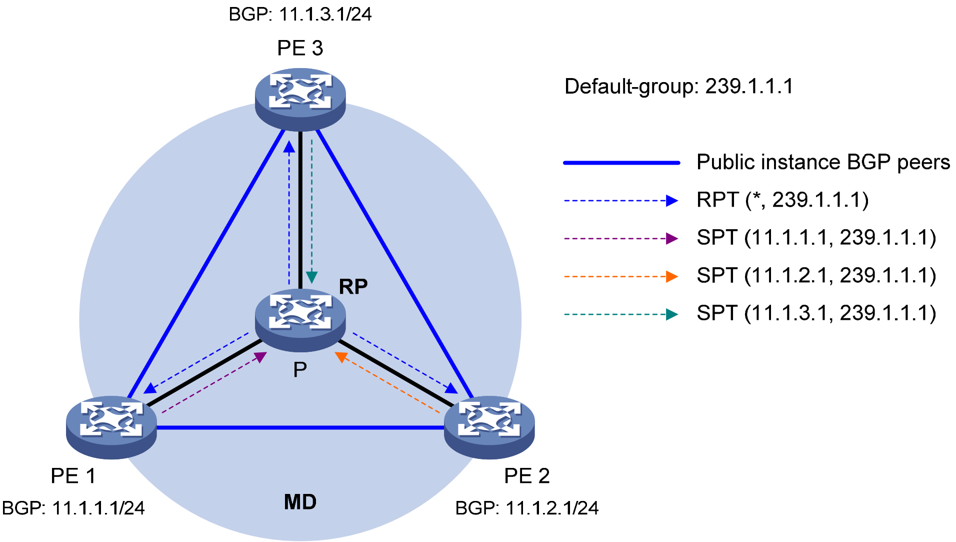
1. To establish PIM neighboring relationships with PE 2 and PE 3 through the MTI in VPN instance A, PE 1 encapsulates the PIM protocol packet of the private network into a public network multicast data packet by specifying the source address as the IP address of the MD source interface and the multicast group address as the default-group address, and then send it to the public network.

   With other PE devices that support VPN instance A as default-group members, PE 1 of VPN instance A initiates a flood-prune process in the entire public network and a (11.1.1.1, 239.1.1.1) state entry is created on each device along the path on the public network. This forms an SPT with PE 1 as the root, and PE 2 and PE 3 as leaves.
2. At the same time, PE 2 and PE 3 separately initiate a similar flood-prune process.

   Finally, three independent SPTs are established in the MD, constituting a default-MDT in the PIM-DM network.

Default-MDT establishment in a PIM-SM network

Figure 61 Default-MDT establishment in a PIM-SM network



As shown in Figure 61, PIM-SM is enabled in the network and all the PE devices support VPN instance A. The process of establishing a default-MDT is as follows:

1. The public network interface of PE 1 initiates a join to the public network RP by specifying the multicast group address as the default-group address in the join message, and a (*, 239.1.1.1) state entry is created on each device along the path on the public network.
2. At the same time, PE 2 and PE 3 separately 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.
3. To establish PIM neighboring relationships with PE 2 and PE 3 through the MTI in VPN instance A, PE 1 encapsulates the PIM protocol packet of the private network into a public network multicast data packet by specifying the source address as the IP address of the MD source interface and the multicast group address as the default-group address, and then send it to the public network. The public network interface of PE 1 first registers the multicast source with the public network RP and the public network RP initiates a join to PE 1. A (11.1.1.1, 239.1.1.1) state entry is created on each device along the path on the public network.
4. At the same time, PE 2 and PE 3 separately 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, or the (*, 239.1.1.1) tree, and the three independent SPTs constitute a default-MDT.

Default-MDT characteristics

No matter what PIM mode is running on the public network, the default-MDT has the following characteristics:

- All PE devices that support the same VPN instance join the default-MDT.
- All VPN multicast packets that belong to this VPN are forwarded along the default-MDT to every PE device on the public network, even if they have no active receivers downstream.

Default-MDT-based delivery

The default-MDT delivers multicast protocol packets and multicast data packets differently.

Multicast protocol packet delivery

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 default-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 different circumstances:

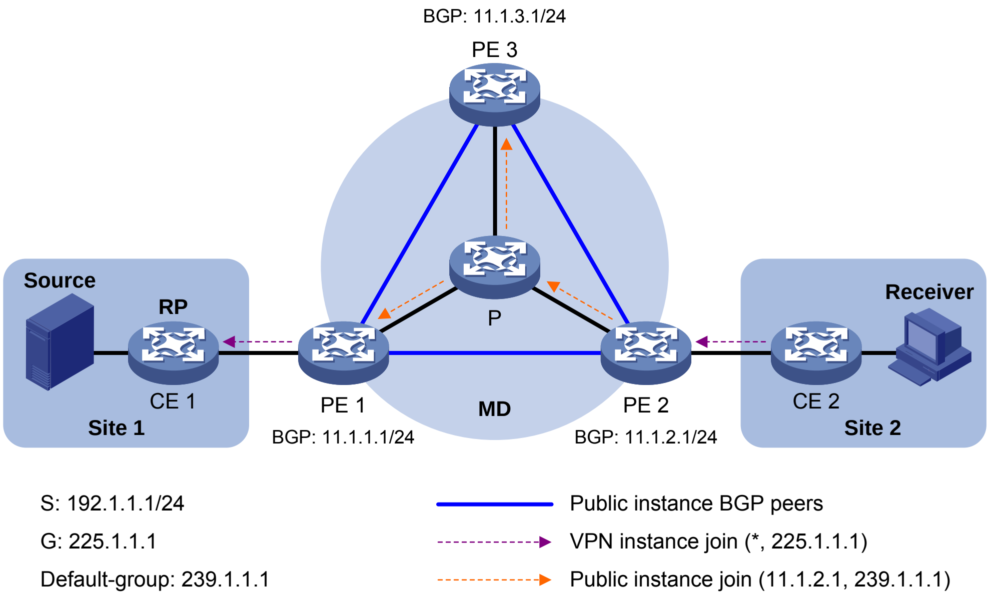
- If the VPN network runs PIM-DM or PIM-SSM:
  - Hello packets are forwarded through MTI interfaces to establish PIM neighboring relationships.
  - A flood-prune process (in PIM-DM) or a join process (in PIM-SSM) is initiated across the public network to establish an SPT across the public network.
- If the VPN network runs PIM-SM:
  - Hello packets are forwarded through 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.

NOTE:

PIM mode must be the same for all interfaces that belong to the same VPN, including those interfaces that are bound with the VPN instance and the MTI interfaces on PE devices.

As shown in Figure 62, 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 default-group address used to forward public network data is 239.1.1.1.

Figure 62 Transmission of multicast protocol packets



The multicast protocol packet is delivered as follows:

1. Receiver sends an IGMP report to CE 2 to join the multicast group G. CE 2 creates a local state entry (*, 225.1.1.1) and sends a join message to the VPN RP (CE 1).
2. After receiving the join message from CE 2, the VPN instance on PE 2 creates a state entry (*, 225.1.1.1) and specify the MTI interface as the upstream interface. The VPN instance on PE 2 considers that the join message has been sent out of the MTI interface because step 3 is transparent to the VPN instance.
3. PE 2 encapsulates the join message into a public network multicast data packet (11.1.2.1, 239.1.1.1) by using the GRE method. The source address of this public network multicast data packet is the MD source interface IP address 11.1.2.1, and the destination address is the default-group address 239.1.1.1. PE 2 then forwards this packet to the public network.
4. The default-MDT forwards the multicast data packet (11.1.2.1, 239.1.1.1) to the public network instance on all the PE devices. After receiving this packet, every PE device decapsulates it to get the original join message to be sent to the VPN RP. Then, each PE device examines the VPN RP address in the join message. If the VPN RP is in the site to which a PE device is connected, 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 the received message is from the MTI. PE 1 creates a local state entry (*, 225.1.1.1), 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. After receiving the join message from the VPN instance on PE 1, CE 1 creates a local state entry (*, 225.1.1.1) or updates the entry if it already exists.

By now, the construction of an RPT across the public network is completed.

Multicast data packet delivery

After the default-MDT is established, the multicast source forwards the VPN multicast data to the receivers in each site along the default-MDT. The VPN multicast packets are encapsulated into public network multicast packets on the local PE device, transmitted along the default-MDT, and then decapsulated on the remote PE device and transmitted in that VPN site.

VPN multicast data packets are forwarded across the public network differently in the following circumstances:

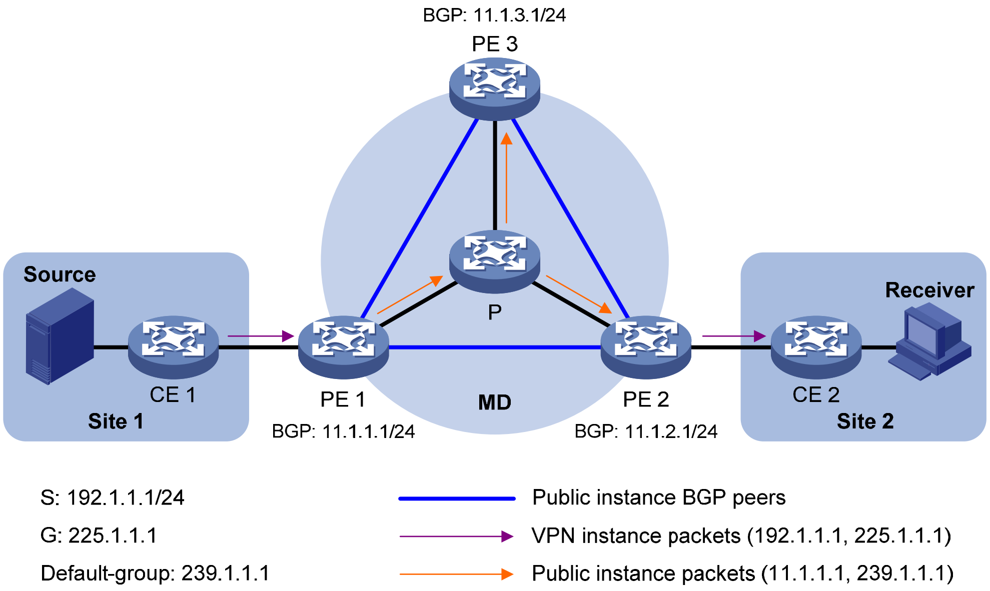
1. If PIM-DM or PIM-SSM is running in the VPN, the multicast source forwards multicast data packets to the receivers along the VPN SPT across the public network.
2. When PIM-SM is running in the VPN:
   - Before the RPT-to-SPT switchover, if the multicast source and the VPN RP are in different sites, the multicast source forwards VPN multicast data packets to the VPN RP along the VPN SPT across the public network. If the VPN RP and the receivers are in different sites, the VPN RP forwards VPN multicast data packets to the receivers along the VPN RPT over the public network.
   - After the RPT-to-SPT switchover, if the multicast source and the receivers are in different sites, the multicast source forwards VPN multicast data packets to the receivers along the VPN SPT across the public network.

   For more information about RPT-to-SPT switchover, see "Configuring PIM."

The following example explains how multicast data packets are delivered based on the default-MDT when PIM-DM is running in both the public network and the VPN network.

As shown in Figure 63, 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 default-group address used to forward public network multicast data is 239.1.1.1.

Figure 63 Multicast data packet delivery



A VPN multicast data packet is delivered across the public network as follows:

3. Source sends a VPN multicast data packet (192.1.1.1, 225.1.1.1) to CE 1.
4. CE 1 forwards the VPN multicast data packet along an SPT to PE 1, and the VPN instance on PE 1 examines the MVRF.

   If the outgoing interface list of the forwarding entry contains an MTI, PE 1 processes the VPN multicast data packet as described in step 3. The VPN instance on PE 1 considers that the VPN multicast data packet has been sent out of the MTI because step 3 is transparent to it.

5. PE 1 encapsulates the VPN multicast data packet into a public network multicast packet (11.1.1.1, 239.1.1.1) by using the GRE method. The source IP address of the packet is the MD source interface 11.1.1.1 and the destination address is the default-group address 239.1.1.1. PE 1 then forwards it to the public network.
6. The default-MDT forwards the multicast data packet (11.1.1.1, 239.1.1.1) to the public network instance on all the PE devices. After receiving this packet, every PE device decapsulates it to get the original VPN multicast data packet, and passes it to the corresponding VPN instance. If a PE device 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 looks up the MVRF and finally delivers the VPN multicast data to Receiver.

   By now, the process of transmitting a VPN multicast data packet across the public network is completed.

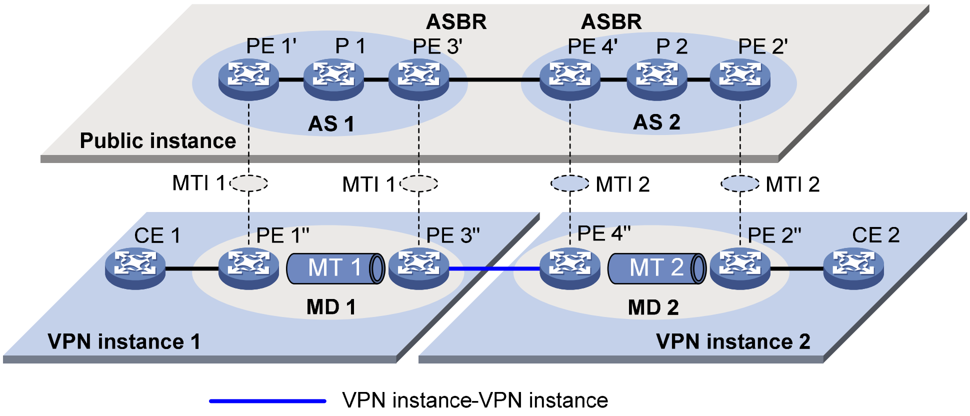
Inter-AS MD VPN

If the nodes of a VPN network are allocated in multiple ASs, these VPN nodes must be interconnected. To implement inter-AS VPN, VRF-to-VRF PE interconnectivity and multi-hop EBGP interconnectivity are available.

VRF-to-VRF PE interconnectivity

As shown in Figure 64, a VPN involves AS 1 and AS 2. PE 3 and PE 4 are ASBRs 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 64 VPN instance-VPN instance interconnectivity



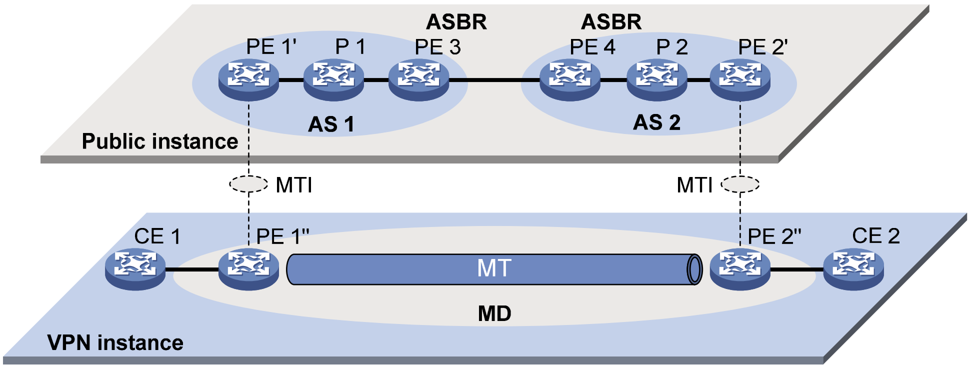
By using this method, a separate MD must be established within each AS, and VPN multicast data traffic between different ASs is transmitted between the two MDs.

Because only VPN multicast data traffic is forwarded between ASBRs, different PIM modes can run within different ASs. However, the same PIM mode 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 65, a VPN network involves AS 1 and AS 2. PE 3 and PE 4 are the ASBRs 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 65 Multi-hop EBGP interconnectivity



By using this method, only one MD needs to be established for all the ASs, and public network multicast traffic between different ASs is transmitted within this MD.

Multicast VPN configuration task list

Task at a glance
(Required.) Enabling IP multicast routing in a VPN instance
(Required.) Creating the MD for a VPN instance
(Required.) Specifying the default-group address
(Required.) Specifying the MD source interface

The MTI interfaces are automatically created and bound with the VPN instance when you create the MD for the VPN instance. Follow these guidelines to make sure the MTI interfaces are correctly created.

- The MTI interfaces take effect only after the default-group is specified and the MD source interface gets the public IP address.
- The PIM mode on the MTI must be the same as the PIM mode running on the VPN instance to which the MTI belongs. When at least one interface on the VPN instance is enabled with PIM, the MTI is enabled with PIM accordingly. When all interfaces on the VPN instance are disabled with PIM, PIM is also disabled on the MTI.

Configuring MD-VPN

This section describes how to configure MD-VPN.

Configuration prerequisites

Before you configure MD-VPN, complete the following tasks:

- Configure a unicast routing protocol on the public network.
- Configure MPLS L3VPN on the public network.
- Configure PIM (PIM-DM, PIM-SM, or PIM-SSM) on the public network.
- Determine the VPN instance names and RDs.

- Determine the default-group addresses.
- Determine the source address for establishing BGP peers.

Enabling IP multicast routing in a VPN instance

Before you configure any MD-VPN functionality for a VPN, you must create a VPN instance and enable IP multicast routing in this VPN instance.

Perform the following configuration on the PE.

To enable IP multicast routing in a VPN instance:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a VPN instance and enter VPN instance view.	**ip vpn-instance** *vpn-instance-name*	By default, no VPN instance exists on the device. For more information about this command, see *MPLS Command Reference*.
3. Configure an RD for the VPN instance.	**route-distinguisher** *route-distinguisher*	By default, no RD is configured for a VPN instance. For more information about this command, see *MPLS Command Reference*.
4. Return to system view.	**quit**	N/A
5. Enable IP multicast routing for the VPN instance and enter MRIB view of this VPN instance.	**multicast routing vpn-instance** *vpn-instance-name*	Disabled by default.

Creating the MD for a VPN instance

You can create one or multiple MDs to provide services for their associated VPN instances on the PE device. When you create the MD for a VPN instance, the system automatically create the MTI interfaces and bind them with the VPN instance.

To create the MD for a VPN instance:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create the MD for the VPN instance and enter MD view.	**multicast-domain vpn-instance** *vpn-instance-name*	By default, no MD exists for a VPN instance.

Specifying the default-group address

The MTI uses the default-group address as the destination address to encapsulate the VPN multicast packets. The default-group address must be the same and unique for the same VPN instance on different

PE devices. The system prompts error if you specify the same default-group address for different VPN instances.

Perform the following configuration on the PE.

To specify the default-group:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter MD view.	**multicast-domain vpn-instance** *vpn-instance-name*	N/A
3.	Specify a default-group address.	**default-group** *group-address*	By default, no default-group address is specified.

Specifying the MD source interface

The MTI uses the IP address of the MD source interface as the source address to encapsulate the VPN multicast packets. The IP address of the MD source interface must be the same as the source address used for establishing BGP peer relationship. Otherwise, correct routing information cannot be obtained.

Perform the following configuration on the PE.

To specify the MD source interface:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter MD view.	**multicast-domain vpn-instance** *vpn-instance-name*	N/A
3.	Specify the MD source interface.	**source** *interface-type interface-number*	By default, no IP address of the MD source interface is specified.

Displaying and maintaining multicast VPN

Execute **display** commands in any view.

Task	Command
Display the default-group information.	**display multicast-domain** [**vpn-instance** *vpn-instance-name*] **default-group**

Multicast VPN configuration examples

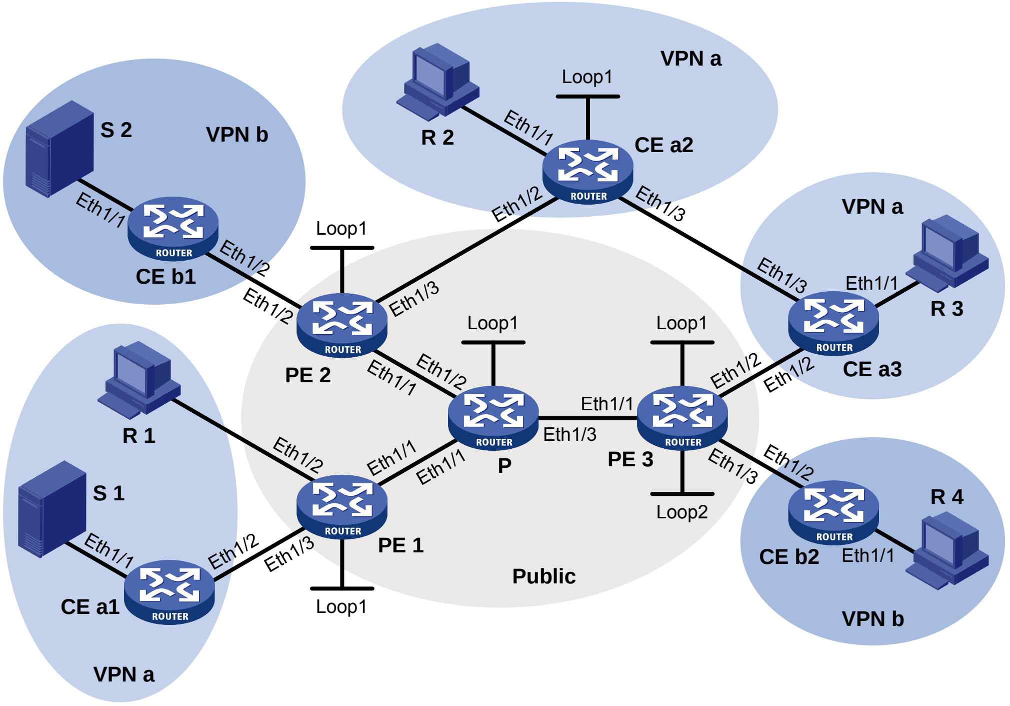
This section provides examples of configuring multicast VPN.

Intra-AS MD VPN configuration example

Network requirements

Item	Network requirements
Multicast sources and receivers	• In VPN instance **a**, S 1 is a multicast source, and R 1, R 2 and R 3 are receivers. • In VPN instance **b**, S 2 is a multicast source, and R 4 is a receiver. • For VPN instance **a**, the default-group address is 239.1.1.1. • For VPN instance **b**, the default-group address is 239.2.2.2.
PE interfaces and VPN instances to which they belong	• PE 1: Ethernet 1/2 and Ethernet 1/3 belong to VPN instance **a**. Ethernet 1/1 and Loopback 1 belong to the public network. • PE 2: Ethernet 1/2 belongs to VPN instance **b**. Ethernet 1/3 belongs to VPN instance **a**. Ethernet 1/1 and Loopback 1 belong to the public network. • PE 3: Ethernet 1/2 belongs to VPN instance **a**. Ethernet 1/3 and Loopback 2 belongs to VPN instance **b**. Ethernet 1/1 and Loopback 1 belong to the public network.
Unicast routing protocols and MPLS	• Configure OSPF on the public network and configure RIP between the PE devices and the CE devices. • Establish BGP peer connections between PE 1, PE 2, and PE 3 on their respective Loopback 1 and exchange all VPN routes between them. • Configure MPLS on the public network.
IP multicast routing	• Enable IP multicast routing on the P router. • Enable IP multicast routing on the public network instance 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 Ethernet 1/2 of PE 1. • Run IGMPv2 on Ethernet 1/1 of CE a2, CE a3, and CE b2.
PIM	• Enable PIM-SM on all interfaces of the P router. • 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 public network C-BSR and C-RP to provide services for all multicast groups. • Configure Loopback 1 of CE a2 as a C-BSR and a C-RP for VPN instance **a** to provide services for all multicast groups. • Configure Loopback 2 of PE 3 as a C-BSR and a C-RP for VPN instance **b** to provide services for all multicast groups.

Figure 66 Network diagram



Device	Interface	IP address	Device	Interface	IP address
S 1	—	10.110.7.2/24	PE 3	Eth1/1	192.168.8.1/24
S 2	—	10.110.8.2/24		Eth1/2	10.110.5.1/24
R 1	—	10.110.1.2/24		Eth1/3	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	Eth1/1	10.110.7.1/24
P	Eth1/1	192.168.6.2/24		Eth1/2	10.110.2.2/24
	Eth1/2	192.168.7.2/24	CE a2	Eth1/1	10.110.9.1/24
	Eth1/3	192.168.8.2/24		Eth1/2	10.110.4.2/24
	Loop1	2.2.2.2/32		Eth1/3	10.110.12.1/24
PE 1	Eth1/1	192.168.6.1/24		Loop1	22.22.22.22/32
	Eth1/2	10.110.1.1/24	CE a3	Eth1/1	10.110.10.1/24
	Eth1/3	10.110.2.1/24		Eth1/2	10.110.5.2/24
	Loop1	1.1.1.1/32		Eth1/3	10.110.12.2/24
PE 2	Eth1/1	192.168.7.1/24	CE b1	Eth1/1	10.110.8.1/24
	Eth1/2	10.110.3.1/24		Eth1/2	10.110.3.2/24
	Eth1/3	10.110.4.1/24	CE b2	Eth1/1	10.110.11.1/24
	Loop1	1.1.1.2/32		Eth1/2	10.110.6.2/24

Configuration procedure

1. Configure PE 1:

   # Configure a Router ID globally and enable IP multicast routing on the public network.

```
<PE1> system-view
[PE1] router id 1.1.1.1
[PE1] multicast routing
```

```
[PE1-mrib] quit
```

# Configure an MPLS LSR ID and enable the LDP capability.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-ldp] quit
```

# Create VPN instance **a** and configure an RD and route target attributes 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
[PE1-vpn-instance-a] quit
```

# Enable IP multicast routing in VPN instance **a**.

```
[PE1] multicast routing vpn-instance a
[PE1-mrib-a] quit
```

# Assign an IP address to the public network interface Ethernet 1/1, and enable PIM-SM, MPLS capability, and LDP capability on it.

```
[PE1] interface ethernet 1/1
[PE1-Ethernet1/1] ip address 192.168.6.1 24
[PE1-Ethernet1/1] pim sm
[PE1-Ethernet1/1] mpls enable
[PE1-Ethernet1/1] mpls ldp enable
[PE1-Ethernet1/1] quit
```

# Bind Ethernet 1/2 with VPN instance **a**, assign an IP address to Ethernet 1/2, and enable IGMP and PIM-SM on the interface.

```
[PE1] interface ethernet 1/2
[PE1-Ethernet1/2] ip binding vpn-instance a
[PE1-Ethernet1/2] ip address 10.110.1.1 24
[PE1-Ethernet1/2] igmp enable
[PE1-Ethernet1/2] pim sm
[PE1-Ethernet1/2] quit
```

# Bind Ethernet 1/3 with VPN instance **a**, assign an IP address to Ethernet 1/3, and enable PIM-SM on the interface.

```
[PE1] interface ethernet 1/3
[PE1-Ethernet1/3] ip binding vpn-instance a
[PE1-Ethernet1/3] ip address 10.110.2.1 24
[PE1-Ethernet1/3] pim sm
[PE1-Ethernet1/3] quit
```

# Assign an IP address to Loopback 1 and enable PIM-SM on this interface.

```
[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] ip vpn-instance a
[PE1-bgp-a] address-family ipv4
[PE1-bgp-ipv4-a] import-route rip 2
[PE1-bgp-ipv4-a] import-route direct
[PE1-bgp-ipv4-a] quit
[PE1-bgp-a] quit
[PE1–bgp] address-family vpnv4
[PE1–bgp-vpnv4] peer vpn-g enable
[PE1–bgp-vpnv4] quit
[PE1–bgp] quit
```

# Create MD for VPN instance **a** and specify the default-group address and the MD source interface address for it.

```
[PE1] multicast-domain vpn-instance a
[PE1-md-a] default-group 239.1.1.1
[PE1-md-a] source loopback 1
[PE1-md-a] quit
```

# 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 globally and enable IP multicast routing on the public network.

```
<PE2> system-view
[PE2] router id 1.1.1.2
[PE2] multicast routing
[PE2-mrib] quit
```

# Configure an MPLS LSR ID and enable the LDP capability.

```
[PE2] mpls lsr-id 1.1.1.2
[PE2] mpls ldp
[PE2-ldp] quit
```

# Create VPN instance **b** and configure an RD and route target attributes 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
[PE2-vpn-instance-b] quit
```

# Enable IP multicast routing in VPN instance **b**.

```
[PE2] multicast routing vpn-instance a
```

```
[PE2-mrib-a] quit
```

# Create VPN instance **a** and configure an RD and route target attributes 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
[PE2-vpn-instance-a] quit
```

# Enable IP multicast routing in VPN instance **a**.

```
[PE2] multicast routing vpn-instance a
[PE2-mrib-a] quit
```

# Assign an IP address to the public network interface Ethernet 1/1, and enable PIM-SM, MPLS capability, and LDP capability on it.

```
[PE2] interface ethernet 1/1
[PE2-Ethernet1/1] ip address 192.168.7.1 24
[PE2-Ethernet1/1] pim sm
[PE2-Ethernet1/1] mpls enable
[PE2-Ethernet1/1] mpls ldp enable
[PE2-Ethernet1/1] quit
```

# Bind Ethernet 1/2 with VPN instance **b,** assign an IP address to Ethernet 1/2, and enable PIM-SM on the interface.

```
[PE2] interface ethernet 1/2
[PE2-Ethernet1/2] ip binding vpn-instance b
[PE2-Ethernet1/2] ip address 10.110.3.1 24
[PE2-Ethernet1/2] pim sm
[PE2-Ethernet1/2] quit
```

# Bind Ethernet 1/3 with VPN instance **a**, assign an IP address to Ethernet 1/3, and enable PIM-SM on the interface.

```
[PE2] interface ethernet 1/3
[PE2-Ethernet1/3] ip binding vpn-instance a
[PE2-Ethernet1/3] ip address 10.110.4.1 24
[PE2-Ethernet1/3] pim sm
[PE2-Ethernet1/3] quit
```

# Assign an IP address to Loopback 1 and enable PIM-SM on this interface.

```
[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] ipv vpn-instance a
[PE2-bgp-a] address-family ipv4
[PE2-bgp-ipv4-a] import-route rip 2
[PE2-bgp-ipv4-a] import-route direct
```

```
[PE2-bgp-ipv4-a] quit
[PE2-bgp-a] quit
[PE2–bgp] ip vpn-instance b
[PE2-bgp-b] address-family ipv4
[PE2-bgp-ipv4-b] import-route rip 3
[PE2-bgp-ipv4-b] import-route direct
[PE2-bgp-ipv4-b] quit
[PE2-bgp-b] quit
[PE2–bgp] address-family vpnv4
[PE2–bgp-vpnv4] peer vpn-g enable
[PE2–bgp-vpnv4] quit
[PE2–bgp] quit
```

# Create the MD for VPN instance **a** and specify the default-group address and the MD source interface address for it.

```
[PE2] multicast-domain vpn-instance a
[PE2-md-a] default-group 239.1.1.1
[PE2-md-a] source loopback 1
[PE2-md-a] quit
```

# Create the MD for VPN instance **b** and specify the default-group address and the MD source interface address for it.

```
[PE2] multicast-domain vpn-instance b
[PE2-md-b] default-group 239.2.2.2
[PE2-md-b] source loopback 1
[PE2-md-b] 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 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 globally and enable IP multicast routing on the public network.

   ```
   <PE3> system-view
   [PE3] router id 1.1.1.3
   [PE3] multicast routing
   [PE3-mrib] quit
   ```

   # Configure an MPLS LSR ID and enable the LDP capability.

```
[PE3] mpls lsr-id 1.1.1.3
[PE3] mpls ldp
[PE3-ldp] quit
```

# Create VPN instance **a** and configure an RD and route target attributes 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
[PE3-vpn-instance-a] quit
```

# Enable IP multicast routing in VPN instance **a**.

```
[PE3] multicast routing vpn-instance a
[PE3-mrib-a] quit
```

# Create VPN instance **b** and configure an RD and route target attributes 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
[PE3-vpn-instance-b] quit
```

# Enable IP multicast routing in VPN instance **b**.

```
[PE3] multicast routing vpn-instance b
[PE3-mrib-b] quit
```

# Assign an IP address to the public network interface Ethernet 1/1, and enable PIM-SM, MPLS capability, and LDP capability on it.

```
[PE3] interface ethernet 1/1
[PE3-Ethernet1/1] ip address 192.168.8.1 24
[PE3-Ethernet1/1] pim sm
[PE3-Ethernet1/1] mpls enable
[PE3-Ethernet1/1] mpls ldp enable
[PE3-Ethernet1/1] quit
```

# Bind Ethernet 1/2 with VPN instance **a**, assign an IP address to Ethernet 1/2, and enable PIM-SM on the interface.

```
[PE3] interface ethernet 1/2
[PE3-Ethernet1/2] ip binding vpn-instance a
[PE3-Ethernet1/2] ip address 10.110.5.1 24
[PE3-Ethernet1/2] pim sm
[PE3-Ethernet1/2] quit
```

# Bind Ethernet 1/3 with VPN instance **b**, assign an IP address to Ethernet 1/3, and enable PIM-SM on the interface.

```
[PE3] interface ethernet 1/3
[PE3-Ethernet1/3] ip binding vpn-instance b
[PE3-Ethernet1/3] ip address 10.110.6.1 24
[PE3-Ethernet1/3] pim sm
[PE3-Ethernet1/3] quit
```

# Assign an IP address to Loopback 1 and enable PIM-SM on this interface.

```
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 1.1.1.3 32
[PE3-LoopBack1] pim sm
```

```
[PE3-LoopBack1] quit
```

# Bind Loopback 2 with VPN instance **b**, assign an IP address to Loopback 2, 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 C-RP for VPN instance **b**.

```
[PE3] pim vpn-instance b
[PE3-pim-b] c-bsr 33.33.33.33
[PE3-pim-b] c-rp 33.33.33.33
[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] ip vpn-instance a
[PE3-bgp-a] address-family ipv4
[PE3-bgp-ipv4-a] import-route rip 2
[PE3-bgp-ipv4-a] import-route direct
[PE3-bgp-ipv4-a] quit
[PE3-bgp-a] quit
[PE3–bgp] ip vpn-instance b
[PE3-bgp-b] address-family ipv4
[PE3-bgp-ipv4-b] import-route rip 3
[PE3-bgp-ipv4-b] import-route direct
[PE3-bgp-ipv4-b] quit
[PE3-bgp-b] quit
[PE3–bgp] address-family vpnv4
[PE3–bgp-vpnv4] peer vpn-g enable
[PE3–bgp-vpnv4] quit
[PE3–bgp] quit
```

# Create MD for VPN instance **a** and specify the default-group address and the MD source interface address.

```
[PE3] multicast-domain vpn-instance a
[PE3-md-a] default-group 239.1.1.1
[PE3-md-a] source loopback 1
[PE3-md-a] quit
```

# Create MD for VPN instance **b** and specify the default-group address and the MD source interface address.

```
[PE3] multicast-domain vpn-instance b
[PE3-md-b] default-group 239.2.2.2
[PE3-md-b] source loopback 1
[PE3-md-b] 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 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. Configuring the P router:

# Enable IP multicast routing on the public network.

```
<P> system-view
[P] multicast routing
[P-mrib] quit
```

# Configure an MPLS LSR ID and enable the LDP capability.

```
[P] mpls lsr-id 2.2.2.2
[P] mpls ldp
[P-ldp] quit
```

# Assign an IP address to the public network interface Ethernet 1/1, and enable PIM-SM, MPLS capability, and LDP capability on it.

```
[P] interface ethernet 1/1
[P-Ethernet1/1] ip address 192.168.6.2 24
[P-Ethernet1/1] pim sm
[P-Ethernet1/1] mpls enable
[P-Ethernet1/1] mpls ldp enable
[P-Ethernet1/1] quit
```

# Assign an IP address to the public network interface Ethernet 1/2, and enable PIM-SM, MPLS capability, and LDP capability on it.

```
[P] interface ethernet 1/2
[P-Ethernet1/2] ip address 192.168.7.2 24
[P-Ethernet1/2] pim sm
[P-Ethernet1/2] mpls enable
[P-Ethernet1/2] mpls ldp enable
[P-Ethernet1/2] quit
```

# Assign an IP address to the public network interface Ethernet 1/3, and enable PIM-SM, MPLS capability, and LDP capability on it.

```
[P] interface ethernet 1/3
[P-Ethernet1/3] ip address 192.168.8.2 24
[P-Ethernet1/3] pim sm
```

```
[P-Ethernet1/3] mpls enable
[P-Ethernet1/3] mpls ldp enable
[P-Ethernet1/3] quit
```

# Assign an IP address to Loopback 1 and enable PIM-SM on the interface.

```
[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 C-RP on the public network.

```
[P] pim
[P-pim] c-bsr 2.2.2.2
[P-pim] c-rp 2.2.2.2
[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
[CEa1-mrib] quit
```

# Assign an IP address to Ethernet 1/1 and enable PIM-SM on it.

```
[CEa1] interface ethernet 1/1
[CEa1-Ethernet1/1] ip address 10.110.7.1 24
[CEa1-Ethernet1/1] pim sm
[CEa1-Ethernet1/1] quit
```

# Assign an IP address to Ethernet 1/2 and enable PIM-SM on it.

```
[CEa1] interface ethernet 1/2
[CEa1-Ethernet1/2] ip address 10.110.2.2 24
[CEa1-Ethernet1/2] pim sm
[CEa1-Ethernet1/2] 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
[CEb1-mrib] quit
```

# Assign an IP address to Ethernet 1/1 and enable PIM-SM on it.

```
[CEb1] interface ethernet 1/1
[CEb1-Ethernet1/1] ip address 10.110.8.1 24
[CEb1-Ethernet1/1] pim sm
[CEb1-Ethernet1/1] quit
```

# Assign an IP address to Ethernet 1/2 and enable PIM-SM on it.

```
[CEb1] interface ethernet 1/2
[CEb1-Ethernet1/2] ip address 10.110.3.2 24
[CEb1-Ethernet1/2] pim sm
[CEb1-Ethernet1/2] 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
[CEa2-mrib] quit
```

# Assign an IP address to Ethernet 1/1 and enable IGMP and PIM-SM on it.

```
[CEa2] interface ethernet 1/1
[CEa2-Ethernet1/1] ip address 10.110.9.1 24
[CEa2-Ethernet1/1] igmp enable
[CEa2-Ethernet1/1] pim sm
[CEa2-Ethernet1/1] quit
```

# Assign an IP address to Ethernet 1/2 and enable PIM-SM on it.

```
[CEa2] interface ethernet 1/2
[CEa2-Ethernet1/2] ip address 10.110.4.2 24
[CEa2-Ethernet1/2] pim sm
[CEa2-Ethernet1/2] quit
```

# Assign an IP address to Ethernet 1/3 and enable PIM-SM on it.

```
[CEa2] interface ethernet 1/3
[CEa2-Ethernet1/3] ip address 10.110.12.1 24
[CEa2-Ethernet1/3] pim sm
[CEa2-Ethernet1/3] quit
```

# Assign an IP address to Loopback 1 and enable PIM-SM on the interface.

```
[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 BSR and a RP for VPN instance **a**.

```
[CEa2] pim
[CEa2-pim] c-bsr 22.22.22.22
[CEa2-pim] c-rp 22.22.22.22
[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
[CEa3-mrib] quit
```

# Assign an IP address to Ethernet 1/1, and enable IGMP and PIM-SM on it.

```
[CEa3] interface ethernet 1/1
[CEa3-Ethernet1/1] ip address 10.110.10.1 24
[CEa3-Ethernet1/1] igmp enable
[CEa3-Ethernet1/1] pim sm
[CEa3-Ethernet1/1] quit
```

# Assign an IP address to Ethernet 1/2 and enable PIM-SM on it.

```
[CEa3] interface ethernet 1/2
[CEa3-Ethernet1/2] ip address 10.110.5.2 24
[CEa3-Ethernet1/2] pim sm
[CEa3-Ethernet1/2] quit
```

# Assign an IP address to Ethernet 1/3 and enable PIM-SM on it.

```
[CEa3] interface ethernet 1/3
[CEa3-Ethernet1/3] ip address 10.110.12.2 24
[CEa3-Ethernet1/3] pim sm
[CEa3-Ethernet1/3] 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
[CEb2-mrib] quit
```

# Assign an IP address to Ethernet 1/1, and enable IGMP and PIM-SM on it.

```
[CEb2] interface ethernet 1/1
[CEb2-Ethernet1/1] ip address 10.110.11.1 24
[CEb2-Ethernet1/1] igmp enable
[CEb2-Ethernet1/1] pim sm
[CEb2-Ethernet1/1] quit
```

# Assign an IP address to Ethernet 1/2 and enable PIM-SM on it.

```
[CEb2] interface ethernet 1/2
[CEb2-Ethernet1/2] ip address 10.110.6.2 24
[CEb2-Ethernet1/2] pim sm
[CEb2-Ethernet1/2] quit
```

# Configure RIP.

```
[CEb2] rip 3
[CEb2-rip-3] network 10.0.0.0
```

Verifying the configuration

Use the **display multicast-domain default-group** command to display the default-group information.

# Display information about the default-groups in VPN instances on PE 1.

```
[PE1] display multicast-domain default-group
 Group address     Source address    Interface     VPN instance
 239.1.1.1        1.1.1.1          MTunnel0      a
```

# Display information about the default-groups in VPN instances on PE 2.

```
[PE2] display multicast-domain default-group
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.2          MTunnel0      a
 239.1.1.1        1.1.1.2          MTunnel1      b
```

# Display information about the default-groups in VPN instances on PE 3.

```
[PE3] display multicast-domain default-group
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.3          MTunnel0      a
 239.2.2.2        1.1.1.3          MTunnel1      b
```

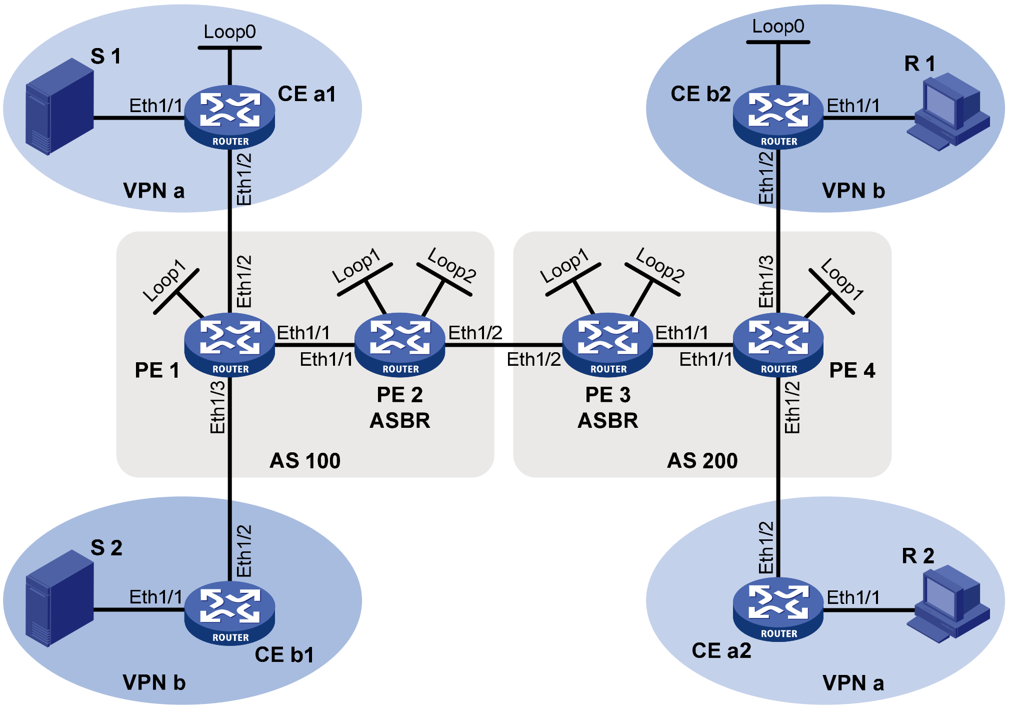
Inter-AS MD VPN configuration example

Network requirements

Item	Network requirements
Multicast sources and receivers	• In VPN instance **a**, S 1 is a multicast source, and R 2 is a receiver. • In VPN instance **b**, S 2 is a multicast source, and R 1 is a receiver. • For VPN instance **a**, the default-group address is 239.1.1.1. • For VPN instance **b**, the default-group address is 239.4.4.4.
PE interfaces and VPN instances to which they belong	• PE 1: Ethernet 1/2 belongs to VPN instance **a**. Ethernet 1/3 belongs to VPN instance **b**. Ethernet 1/1 and Loopback 1 belong to the public network instance. • PE 2: Ethernet 1/1, Ethernet 1/2, Loopback 1, and Loopback 2 belong to the public network instance. • PE 3: Ethernet 1/1, Ethernet 1/2, Loopback 1, and Loopback 2 belong to the public network instance. • PE 4: Ethernet 1/2 belongs to VPN instance **a**. Ethernet 1/3 belongs to VPN instance **b**. Ethernet 1/1 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 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.

Item	Network requirements
IGMP	• Run IGMPv2 on Ethernet 1/1 of CE a2. • Run IGMPv2 on Ethernet 1/1 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 own AS to provide services for all multicast groups. • Configure Loopback 0 of CE a1 as a C-BSR and a C-RP for VPN instance **a** to provide services for all multicast groups. • Configure Loopback 0 of CE b1 as a C-BSR and a C-RP for VPN instance **b** to provide services for all multicast groups.

Figure 67 Network diagram



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	Eth1/1	10.10.1.1/24	PE 3	Eth1/1	10.10.2.1/24
	Eth1/2	10.11.1.1/24		Eth1/2	192.168.1.2/24
	Eth1/3	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	Eth1/1	10.10.1.2/24	PE 4	Eth1/1	10.10.2.2/24
	Eth1/2	192.168.1.1/24		Eth1/2	10.11.3.1/24
	Loop1	1.1.1.2/32		Eth1/3	10.11.4.1/32
	Loop2	11.11.11.11/32		Loop2	1.1.1.4/32
CE a1	Eth1/1	10.11.5.1/24	CE b1	Eth1/1	10.11.6.1/24
	Eth1/2	10.11.1.2/24		Eth1/2	10.11.2.2/24
	Loop0	2.2.2.2/32	CE b2	Eth1/1	10.11.8.1/24
CE a2	Eth1/1	10.11.7.1/24		Eth1/2	10.11.4.2/24
	Eth1/2	10.11.3.2/24		Loop0	3.3.3.3/32

Configuration procedure

1. Configure PE 1:

# Configure a Router ID and enable IP multicast routing on the public network.

```
<PE1> system-view
[PE1] router id 1.1.1.1
[PE1] multicast routing
[PE1-mrib] quit
```

# Configure an MPLS LSR ID and enable the LDP capability.

```
[PE1] mpls lsr-id 1.1.1.1
```

```
[PE1] mpls ldp
[PE1-ldp] quit
```

# Create VPN instance **a** and configure an RD and route target attributes 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
[PE1-vpn-instance-a] quit
```

# Enable IP multicast routing in VPN instance **a**.

```
[PE1] multicast routing vpn-instance a
[PE1-mrib-a] quit
```

# Create VPN instance **b** and configure an RD and route target attributes for it.

```
[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] quit
```

# Enable IP multicast routing in VPN instance **b**.

```
[PE1] multicast routing vpn-instance b
[PE1-mrib-b] quit
```

# Assign an IP address to the public network interface Ethernet 1/1, and enable PIM-SM, MPLS capability, and LDP capability on it.

```
[PE1] interface ethernet 1/1
[PE1-Ethernet1/1] ip address 10.10.1.1 24
[PE1-Ethernet1/1] pim sm
[PE1-Ethernet1/1] mpls enable
[PE1-Ethernet1/1] mpls ldp enable
[PE1-Ethernet1/1] quit
```

# Bind Ethernet 1/2 with VPN instance **a**, assign an IP address to Ethernet 1/2**,** and enable PIM-SM on the interface.

```
[PE1] interface ethernet 1/2
[PE1-Ethernet1/2] ip binding vpn-instance a
[PE1-Ethernet1/2] ip address 10.11.1.1 24
[PE1-Ethernet1/2] pim sm
[PE1-Ethernet1/2] quit
```

# Bind Ethernet 1/3 with VPN instance **b**, assign an IP address to Ethernet 1/3, and enable PIM-SM on the interface.

```
[PE1] interface ethernet 1/3
[PE1-Ethernet1/3] ip binding vpn-instance b
[PE1-Ethernet1/3] ip address 10.11.2.1 24
[PE1-Ethernet1/3] pim sm
[PE1-Ethernet1/3] quit
```

# Assign an IP address to Loopback 1 and enable PIM-SM on the interface.

```
[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-pe4 connect-interface loopback 1
[PE1–bgp] ip vpn-instance a
[PE1-bgp-a] address-family ipv4
[PE1-bgp-ipv4-a] import-route ospf 2
[PE1-bgp-ipv4-a] import-route direct
[PE1-bgp-ipv4-a] quit
[PE1-bgp-a] quit
[PE1–bgp] ip vpn-instance b
[PE1-bgp-b] address-family ipv4
[PE1-bgp-ipv4-b] import-route ospf 3
[PE1-bgp-ipv4-b] import-route direct
[PE1-bgp-ipv4-b] quit
[PE1-bgp-b] quit
[PE1–bgp] address-family vpnv4
[PE1–bgp-vpnv4] peer 1.1.1.4 enable
[PE1–bgp-vpnv4] quit
[PE1–bgp] quit
```

# Create the MD for VPN instance **a** and specify the default-group address and the MD source interface address for it.

```
[PE1] multicast-domain vpn-instance a
[PE1-md-a] default-group 239.1.1.1
[PE1-md-a] source loopback 1
[PE1-md-a] quit
```

# Create the MD for VPN instance **b** and specify the default-group address and the MD source interface address for it.

```
[PE1] multicast-domain vpn-instance b
[PE1-md-b] default-group 239.4.4.4
[PE1-md-b] source loopback 1
[PE1-md-b] quit
```

# 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 and enable IP multicast routing on the public network.

   ```
   <PE2> system-view
   [PE2] router id 1.1.1.2
   [PE2] multicast routing
   [PE2-mrib] quit
   ```

   # Configure an MPLS LSR ID and enable the LDP capability.

   ```
   [PE2] mpls lsr-id 1.1.1.2
   [PE2] mpls ldp
   [PE2-mpls-ldp] quit
   ```

   # Assign an IP address to the public network interface Ethernet 1/1, and enable PIM-SM, MPLS capability, and LDP capability on it.

   ```
   [PE2] interface ethernet 1/1
   [PE2-Ethernet1/1] ip address 10.10.1.2 24
   [PE2-Ethernet1/1] pim sm
   [PE2-Ethernet1/1] mpls enable
   [PE2-Ethernet1/1] mpls ldp enable
   [PE2-Ethernet1/1] quit
   ```

   # Assign an IP address to the public network interface Ethernet 1/2, and enable PIM-SM and MPLS on it.

   ```
   [PE2] interface ethernet 1/2
   [PE2-Ethernet1/2] ip address 192.168.1.1 24
   [PE2-Ethernet1/2] pim sm
   [PE2-Ethernet1/2] mpls enable
   [PE2-Ethernet1/2] quit
   ```

   # Assign an IP address to Loopback 1 and enable PIM-SM on this interface.

   ```
   [PE2] interface loopback 1
   [PE2-LoopBack1] ip address 1.1.1.2 32
   [PE2-LoopBack1] pim sm
   [PE2-LoopBack1] quit
   ```

   # Assign an IP address to Loopback 2 and enable PIM-SM on this interface.

   ```
   [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 11.11.11.11
[PE2-pim] c-rp 11.11.11.11
[PE2-pim] quit
```

# Configure BGP.

```
[PE2] bgp 100
[PE2-bgp] address-family ipv4
[PE2-bgp-ipv4] import-route ospf 1
[PE2-bgp-ipv4] quit
[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 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 routing policy.

```
[PE2] route-policy map1 permit node 10
[PE2-route-policy-map1-10] apply mpls-label
[PE2-route-policy-map1-10] quit
[PE2] route-policy map2 permit node 10
[PE2-route-policy-map1-10] if-match mpls-label
[PE2-route-policy-map1-10] apply mpls-label
[PE2-route-policy-map1-10] quit
```

3. Configure PE 3:

# Configure a Router ID and enable IP multicast routing on the public network.

```
<PE3> system-view
[PE3] router id 1.1.1.3
[PE3] multicast routing
[PE3-mrib] quit
```

# Configure an MPLS LSR ID and enable the LDP capability.

```
[PE3] mpls lsr-id 1.1.1.3
[PE3] mpls ldp
[PE3-ldp] quit
```

# Assign an IP address to the public network interface Ethernet 1/1, and enable PIM-SM, MPLS capability, and LDP capability on it.

```
[PE3] interface ethernet 1/1
[PE3-Ethernet1/1] ip address 10.10.2.1 24
[PE3-Ethernet1/1] pim sm
[PE3-Ethernet1/1] mpls enable
[PE3-Ethernet1/1] mpls ldp enable
[PE3-Ethernet1/1] quit
```

# Assign an IP address to the public network interface Ethernet 1/2, and enable PIM-SM and MPLS on it.

```
[PE3] interface ethernet 1/2
[PE3-Ethernet1/2] ip address 192.168.1.2 24
[PE3-Ethernet1/2] pim sm
[PE3-Ethernet1/2] mpls enable
[PE3-Ethernet1/2] quit
```

# Assign an IP address to Loopback 1 and enable PIM-SM on this interface.

```
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 1.1.1.3 32
[PE3-LoopBack1] pim sm
[PE3-LoopBack1] quit
```

# Assign an IP address to Loopback 2 and enable PIM-SM on this interface.

```
[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 22.22.22.22
[PE3-pim] c-rp 22.22.22.22
[PE3-pim] quit
```

# Configure BGP.

```
[PE3] bgp 200
[PE2-bgp] address-family ipv4
[PE3-bgp-ipv4] import-route ospf 1
[PE3-bgp-ipv4] quit
[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 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 routing policy.

```
[PE3] route-policy map1 permit node 10
[PE3-route-policy-map1-10] apply mpls-label
[PE3-route-policy-map1-10] quit
[PE3] route-policy map2 permit node 10
[PE3-route-policy-map2-10] if-match mpls-label
[PE3-route-policy-map2-10] apply mpls-label
[PE3-route-policy-map2-10] quit
```

4. Configure PE 4:

# Configure a Router ID and enable IP multicast routing on the public network.

```
<PE4> system-view
[PE4] router id 1.1.1.4
[PE4] multicast routing
[PE4-mrib] quit
```

# Configure an MPLS LSR ID and enable the LDP capability.

```
[PE4] mpls lsr-id 1.1.1.4
[PE4] mpls ldp
[PE4-ldp] quit
```

# Create VPN instance **a** and configure an RD and route target attributes for it.

```
[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] quit
```

# Enable IP multicast routing in VPN instance **a**.

```
[PE4] multicast routing vpn-instance a
[PE4-mrib-a] quit
```

# Create VPN instance **b** and configure an RD and route target attributes for it.

```
[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] quit
```

# Enable IP multicast routing in VPN instance **b**.

```
[PE4] multicast routing vpn-instance b
[PE4-mrib-b] quit
```

# Assign an IP address to the public network interface Ethernet 1/1, and enable PIM-SM, MPLS capability, and LDP capability on it.

```
[PE4] interface ethernet 1/1
[PE4-Ethernet1/1] ip address 10.10.2.2 24
[PE4-Ethernet1/1] pim sm
[PE4-Ethernet1/1] mpls enable
[PE4-Ethernet1/1] mpls ldp enable
[PE4-Ethernet1/1] quit
```

# Bind Ethernet 1/2 with VPN instance **a**, assign an IP address to Ethernet 1/2, and enable PIM-SM on the interface.

```
[PE4] interface ethernet 1/2
[PE4-Ethernet1/2] ip binding vpn-instance a
[PE4-Ethernet1/2] ip address 10.11.3.1 24
[PE4-Ethernet1/2] pim sm
[PE4-Ethernet1/2] quit
```

# Bind Ethernet 1/3 with VPN instance **b**, assign an IP address to Ethernet 1/3, and enable PIM-SM on the interface.

```
[PE4] interface ethernet 1/3
[PE4-Ethernet1/3] ip binding vpn-instance b
[PE4-Ethernet1/3] ip address 10.11.4.1 24
[PE4-Ethernet1/3] pim sm
[PE4-Ethernet1/3] quit
```

# Assign an IP address to Loopback 1 and enable PIM-SM on this interface.

```
[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] ip vpn-instance a
[PE4-bgp-a] address-family ipv4
[PE4-bgp-ipv4-a] import-route ospf 2
[PE4-bgp-ipv4-a] import-route direct
[PE4-bgp-ipv4-a] quit
[PE4-bgp-a] quit
[PE4–bgp] ip vpn-instance b
[PE4-bgp-b] address-family ipv4
[PE4-bgp-ipv4-b] import-route ospf 3
[PE4-bgp-ipv4-b] import-route direct
[PE4-bgp-ipv4-b] quit
[PE4-bgp-b] quit
```

```
[PE4–bgp] address-family vpnv4
[PE4–bgp-vpnv4] peer 1.1.1.1 enable
[PE4–bgp-vpnv4] quit
[PE4–bgp] quit
```

# Create the MD for VPN instance **a** and specify the default-group address and the MD source interface address for it.

```
[PE4] multicast-domain vpn-instance a
[PE4-md-a] default-group 239.1.1.1
[PE4-md-a] source loopback 1
[PE4-md-a] quit
```

# Create the MD for VPN instance **b** and specify the default-group address and the MD source interface address for it.

```
[PE4] multicast-domain vpn-instance b
[PE4-md-b] default-group 239.4.4.4
[PE4-md-b] source loopback 1
[PE4-md-b] quit
```

# 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
[CEa1-mrib] quit
```

# Assign an IP address to Ethernet 1/1 and enable PIM-SM on this interface.

```
[CEa1] interface ethernet 1/1
[CEa1-Ethernet1/1] ip address 10.11.5.1 24
[CEa1-Ethernet1/1] pim sm
[CEa1-Ethernet1/1] quit
```

# Assign an IP address to Ethernet 1/2 and enable PIM-SM on this interface.

```
[CEa1] interface ethernet 1/2
```

```
[CEa1-Ethernet1/2] ip address 10.11.1.2 24
[CEa1-Ethernet1/2] pim sm
[CEa1-Ethernet1/2] quit
```

# Assign an IP address to Loopback 1 and enable PIM-SM on this interface.

```
[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 instance **a**.

```
[CEa1] pim
[CEa1-pim] c-bsr 2.2.2.2
[CEa1-pim] c-rp 2.2.2.2 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
[CEb1-mrib] quit
```

# Assign an IP address to Ethernet 1/1 and enable PIM-SM on this interface.

```
[CEb1] interface ethernet 1/1
[CEb1-Ethernet1/1] ip address 10.11.6.1 24
[CEb1-Ethernet1/1] pim sm
[CEb1-Ethernet1/1] quit
```

# Assign an IP address to Ethernet 1/2 and enable PIM-SM on this interface.

```
[CEb1] interface ethernet 1/2
[CEb1-Ethernet1/2] ip address 10.11.2.2 24
[CEb1-Ethernet1/2] pim sm
[CEb1-Ethernet1/2] 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
[CEa2-mrib] quit
```

# Assign an IP address to Ethernet 1/1 and enable IGMP and PIM-SM on this interface.

```
[CEa2] interface ethernet 1/1
[CEa2-Ethernet1/1] ip address 10.11.7.1 24
[CEa2-Ethernet1/1] igmp enable
[CEa2-Ethernet1/1] pim sm
[CEa2-Ethernet1/1] quit
```

# Assign an IP address to Ethernet 1/2 and enable PIM-SM on this interface.

```
[CEa2] interface ethernet 1/2
[CEa2-Ethernet1/2] ip address 10.11.3.2 24
[CEa2-Ethernet1/2] pim sm
[CEa2-Ethernet1/2] 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
[CEb2-mrib] quit
```

# Assign an IP address to Ethernet 1/1 and enable IGMP and PIM-SM on this interface.

```
[CEb2] interface ethernet 1/1
[CEb2-Ethernet1/1] ip address 10.11.8.1 24
[CEb2-Ethernet1/1] igmp enable
[CEb2-Ethernet1/1] pim sm
[CEb2-Ethernet1/1] quit
```

# Assign an IP address to Ethernet 1/2 and enable PIM-SM on this interface.

```
[CEb2] interface ethernet 1/2
[CEb2-Ethernet1/2] ip address 10.11.4.2 24
[CEb2-Ethernet1/2] pim sm
[CEb2-Ethernet1/2] quit
```

# Assign an IP address to Loopback 1 and enable PIM-SM on this interface.

```
[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 instance **b**.

```
[CEb2] pim
[CEb2-pim] c-bsr 3.3.3.3
[CEb2-pim] c-rp 3.3.3.3
[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
```

Verifying the configuration

Use the **display multicast-domain default-group** command to display the default-group information.

# Display information about the default-groups in VPN instances on PE 1.

```
[PE1] display multicast-domain default-group
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.1          MTunnel0      a
 239.4.4.4        1.1.1.1          MTunnel1      b
```

# Display information about the default-groups in VPN instances on PE 4.

```
[PE4] display multicast-domain default-group
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.4          MTunnel0      a
 239.4.4.4        1.1.1.4          MTunnel1      b
```

Troubleshooting MD-VPN

This section describes common MD-VPN problems and how to troubleshoot them.

A default-MDT cannot be established

Symptom

The default-MDT cannot be established. PIM neighboring relationship cannot be established between PE devices' interfaces that are in the same VPN instance.

Analysis

- The construction of the default-MDT requires effective MTI interfaces. The MTI interfaces take effect only after the default-group is specified and the MD source interface gets the public IP address.
- On different PE devices, the same default-group must be configured for the same VPN instance. A default-group address uniquely identifies a default-MDT. If different default-group addresses have been configured for a VPN instance on different PE devices, a default-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, so a default-MDT can be correctly built for the VPN instance and PIM neighboring relationship can 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 PIM to obtain correct routing information. Only when at least one interface of the VPN instance is enabled with PIM, PIM can be enabled on the MTI interface. PIM neighboring relationship 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. Use the **display interface** command to examine the MTI interface state and address encapsulation on the MTI.
2. Use the **display multicast-domain default-group** command to verify that the same default-group address has been configured for the same VPN instance on different PE devices.
3. Use the **display pim interface** command 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.
4. Use the **display ip routing-table** command 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.
5. Use the **display bgp peer** command to verify that the BGP peer connections have been correctly configured.

An MVRF cannot be created

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 VPN DR must have a route to the VPN RP. A route to the multicast source is available in the VPN.

Solution

1. Use the **display pim bsr-info** command to verify that the BSR information exists on the public network and VPN instance. If not, verify that a unicast route exists to the BSR.
2. Use the **display pim rp-info** command to examine the RP information. If no RP information is available, verify that a unicast route exists to the RP. Use the **display pim neighbor** command to verify that the PIM adjacencies have correctly established on the public network and the VPN.
3. Use the **ping** command to examine the connectivity between the VPN DR and the VPN RP.

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/wwalerts

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Websites

- HP.com http://www.hp.com
- HP Networking http://www.hp.com/go/networking
- HP manuals http://www.hp.com/support/manuals
- HP download drivers and software http://www.hp.com/support/downloads
- HP software depot http://www.software.hp.com
- HP Education http://www.hp.com/learn

Conventions

This section describes the conventions used in this documentation set.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
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.

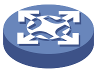
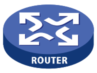
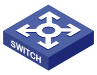
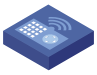
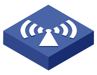
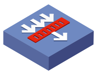
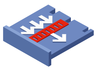
GUI conventions

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.
	Represents an access controller, a unified wired-WLAN module, or the switching engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a security product, such as a firewall, a UTM, or a load-balancing or security card that is installed in a device.
	Represents a security card, such as a firewall card, a load-balancing card, or a NetStream card.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index