# Multicast

## QSR-1920, QSR-2920, QSR-3920

# Оглавление

1. L2 MULTICAST BASICS 1
1.1. Overview 1
1.2. L2 Multicast Basics Function Configuration 1
1.2.1. Configure Unknown Packet Forwarding Policy of L2 Multicast 1
1.2.2. Monitoring and Maintaining of L2 Multicast Basis 2
2. IGMP SNOOPING 1
2.1. Overview 1
2.2. IGMP snooping Function Configuration 1
2.2.1. Configure IGMP snooping Basic Functions 2
2.2.2. Configure IGMP snooping Querier 4
2.2.3. Configure IGMP snooping Router Port 7
2.2.4. Configure IGMP snooping TCN Event 8
2.2.5. Configure IGMP snooping Policy 10
2.2.6. Configure IGMP Snooping Proxy 13
2.2.7. IGMP snooping Monitoring and Maintaining 14
2.3. Typical Configuration Example of IGMP snooping 16
2.3.1. Configure IGMP snooping 16
2.3.2. Configure Multicast Receiving Control 17
2.3.3. Configure IGMP Snooping Proxy 21
3. IPV4 MULTICAST BASICS 25
3.1. Overview 25
3.2. Basic Function Configuration of IPv4 Multicast 25
3.2.1. Enable IP Multicast Forwarding 25
3.2.2. Configure IP Multicast Forwarding Rule 26
3.2.3. Monitoring and Maintaining of IPv4 Multicast Basics 29
4. IGMP 30
4.1. Overview 30
4.2. IGMP Function Configuration 30
4.2.1. Configure IGMP Basic Functions 31
4.2.2. Adjust and Optimize IGMP Network 34
4.2.3. Configure IGMP SSM Mapping 38
4.2.4. Configure IGMP Proxy 39
4.2.5. IGMP Monitoring and Maintaining 40
4.3. IGMP Typical Configuration Example 41
4.3.1. Configure IGMP Basic Functions 41
4.3.2. Configure IGMP Static Adding 43

4.3.3. Configure IGMP SSM Mapping 46
4.3.4. Configure IGMP Multicast Group Filter 53
4.3.5. Configure IGMP Proxying 57
5. PIM-DM 61
5.1. Overview 61
5.2. PIM-DM Function Configuration 61
5.2.1. Configure PIM-DM Basic Functions 61
5.2.2. Configure PIM-DM Neighbor 62
5.2.3. Configure Status Refresh Parameters 64
5.2.4. PIM-DM Monitoring and Maintaining 65
5.3. PIM-DM Typical Configuration Example 65
5.3.1. Configure PIM-DM Basic Functions 65
6. PIM-SM 69
6.1. Overview 69
6.2. PIM-SM Function Configuration 69
6.2.1. Configure PIM-SM Basic Functions 70
6.2.2. Configure PIM-SM Aggregation Router 71
6.2.3. Configure PIM-SM Bootstrap Router 72
6.2.4. Configure PIM-SM Multicast Source Register 74
6.2.5. Configure PIM-SM Neighbor Parameters 76
6.2.6. Configure PIM-SM SPT Switching 78
6.2.7. Configure PIM-SSM 79
6.2.8. Configure PIM Adaptive Basic Function 80
6.2.9. Configure PIM-SM Supporting (*,*,rp) 81
6.2.10. Configure PIM-SM BFD 81
6.2.11. PIM-SM Monitoring and Maintaining 82
6.3. PIM-SM Typical Configuration Example 83
6.3.1. Configure PIM-SM Basic Functions 83
6.3.2. Configure PIM-SSM 92
6.3.3. Configure PIM-SM Multicast Forwarding Control 98
6.3.4. Configure PIM Adaptive Function 107
7. MVPN 115
7.1. Overview 115
7.2. MVPN Function Configuration 115
7.2.1. Configure MVPN Basic Functions 115
7.2.2. Configure RPF Proxy 117
7.2.3. Configure BGP MDT Address Stack 118

7.2.4. MVPN Monitoring and Maintaining 119
7.3. MVPN Typical Configuration Example 119
7.3.1. MVPN Typical Configuration in Single AS 119
7.3.2. Across-AS MVPN Typical Configuration 131
8. NG MVPN 150
8.1. Overview 150
8.2. NG MVPN Function Configuration 150
8.2.1. Configure NG MVPN Basic Functions 151
8.2.2. Configure BGP MVPN Address Family 155
8.2.3. Configure MVPN ORF 156
8.2.4. NG MVPN Monitoring and Maintaining 157
8.3. NG MVPN Typical Configuration Example 159
8.3.1. Configure NG MVPN with the Adding Mode of Private Multicast as (S, G) and Public Tunnel as mLDP P2MP 159
8.3.2. Configure NG MVPN with the Adding Mode of Private Multicast as (S, G) and Public Tunnel as RSVP-TE P2MP 181
8.3.3. Configure S-PMSI Tunnel Switching 203
9. MSDP 224
9.1. Overview 224
9.2. MSDP Function Configuration 224
9.2.1. Configure MSDP Peer 224
9.2.2. Configure MSDP Peer Connection 225
9.2.3. Configure SA Packet 227
9.2.4. MSDP Monitoring and Maintaining 228
9.3. MSDP Typical Configuration Example 229
9.3.1. Configure Inter-PIM-SM Domain Multicast 229
9.3.2. Configure Anycast RP 240
10. MLD 253
10.1. Overview 253
10.2. MLD Function Configuration 253
10.2.1. Configure MLD Basic Functions 253
10.2.2. Adjust and Optimize the MLD Network 256
10.2.3. Configure the MLD SSM Mapping 259
10.2.4. MLD Monitoring and Maintaining 260
10.3. MLD Typical Configuration Example 261
10.3.1. Configure MLD Basic Functions 261
10.3.2. Configure IGMP Static Adding 263
10.3.3. Configure MLD SSM Mapping 266

10.3.4. Configure MLD Multicast Group Filter 272
11. IPV6 MULTICAST BASICS 277
11.1. Overview 277
11.1.1. Enable IPv6 Multicast Forwarding 277
11.1.2. Configure IPV6 Muticast Forwarding Rules 278
Monitoring and Maintaining of IPv6 Multicast Basics 280
12. PIM-SMV6 281
12.1. Overview 281
12.2. PIM-SMv6 Function Configuration 281
12.2.1. Configure PIM-SMv6 Basic Functions 282
12.2.2. Configure PIM-SMv6 Aggregation Router 282
12.2.3. Configure PIM-SMv6 Bootstrap Router 284
12.2.4. Configure PIM-SMv6 Multicast Source Register 285
12.2.5. Configure PIM-SMv6 Neighbor Parameters 288
12.2.6. Configure PIM-SMv6 SPT Switching 290
12.2.7. Configure IPv6 PIM-SSM 291
12.2.8. Configure PIM6-SM BFD 292
12.2.9. PIM-SMv6 Monitoring and Maintaining 292
12.3. PIM-SMv6 Typical Configuration Example 293
12.3.1. Configure PIM-SMv6 Basic Functions 293
12.3.2. Configure IPv6 PIM-SSM 304
12.3.3. Configure PIM-SMv6 Multicast Forwarding Control 311
13. ОБЩАЯ ИНФОРМАЦИЯ 323
13.1. Замечания и предложения 323
13.2. Гарантия и сервис 323
13.3. Техническая поддержка 323
13.4. Электронная версия документа **Ошибка! Закладка не определена.**

# 1. L2 MULTICAST BASICS

## 1.1. Overview

The main task of L2 multicast basis is to maintain the L2 multicast forwarding table. The application modules of L2 multicast generates their L2 multicast tables by static configuration and dynamic learning, and then synchronize the information to the L2 multicast basis modules. L2 multicast basis modules integrate the information to form the L2 multicast forwarding table.

## 1.2. L2 Multicast Basics Function Configuration

Table 1-1 Configuration list of L2 multicast basics

| Configuration Task | |
|---|---|
| Configure the unknown packet forwarding policy of L2 multicast | Configure unknown packet MAC forwarding policy of L2 multicast |

### 1.2.1. Configure Unknown Packet Forwarding Policy of L2 Multicast

Unknown multicast service packets have two kinds of forwarding policies: drop unknown multicast service packets, or make the unknown multicast service packets flood.

**Configuration Condition**

Before configuring the unknown packet forwarding policy of L2 multicast, first complete the following task:

- Configure corresponding VLAN

**Configure Unknown Packet MAC Forwarding Policy of L2 Multicast**

In the L2 multicast MAC forwarding mode, the multicast service packets are forwarded by matching VLAN and destination MAC address. When the multicast service packet does not match the forwarding table, it is unknown multicast service packet. The device has two kinds of forwarding policies for the unknown multicast service packets: drop unknown multicast service packets, or make unknown multicast service packets flood.

Table 1-2 Configure unknown packet MAC forwarding policy of L2 multicast

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter VLAN configuration mode | **vlan** *vlan-id* | - |
| Configure L2 multicast forwarding policy | **l2-multicast drop-unknown** | Optional<br>By default, the function of dropping unknown multicast service packets is not enabled in VLAN. |

### 1.2.2. Monitoring and Maintaining of L2 Multicast Basis

Table 1-3 Monitoring and maintaining of L2 multicast basis

| Command | Description |
|---|---|
| **show l2-multicast ip-entry** | Display the IP forwarding table information of L2 multicast |
| **show l2-multicast l3-ip-entry** | Display the L3 IP forwarding table information of L2 multicast |
| **show l2-multicast mac-entry** { **all** \| **forward** } | Display the L2 multicast table |
| **show l2-multicast vlan-setting { all \|** *vlan-id* **}** | Display the L2 multicast VLAN information |

# 2. IGMP SNOOPING

## 2.1. Overview

IGMP Snooping (Internet Group Management Protocol snooping) is the function designed for the device that does not support IGMP to reduce the spreading range of the multicast service packet and prevent the multicast packet from being spread to the network segments that do not need the multicast packet. It forms and maintains the downstream member port list of each multicast group at the local by listening to IGMP packets. In this way, when receiving multicast service packet, forward at the specified downstream member port. Meanwhile, IGMP Snooping can listen to the IGMP protocol packets and cooperate with the upstream multicast router to manage and control multicast services.

IGMP Snooping mainly realizes the following functions:

- Listen to the IGMP packets to set up multicast information. IGMP Snooping gets the downstream multicast receiver information by listening to IGMP packets, realizing the forwarding of multicast service packets at the specified member port.
- Listen to the IGMP protocol packets. In this way, the upstream multicast router can correctly maintain IGMP member relation table.

## 2.2. IGMP snooping Function Configuration

Table 2-1 IGMP snooping function configuration list

| **Configuration Task** | |
|---|---|
| Configure basic functions of IGMP Snooping | Enable the IGMP Snooping function |
| | Configure the IGMP snooping version |
| | Enable the IGMP snooping L2 forwarding function |
| Configure IGMP snooping querier | Enable the IGMP snooping querier |
| | Configure the source IP address of the IGMP query packet |
| | Configure general group query interval |
| | Configure the maximum response time |
| | Configure the query interval of the specified group |
| | Configure fast-leave |
| Configure IGMP snooping router port | Configure IGMP snooping router port |

| Configuration Task | |
|---|---|
| | Configure the age time of IGMP snooping dynamic router port |
| Configure IGMP snooping TCN event | Enable fast convergence |
| | Configure the query interval of TCN event |
| | Configure the query times of TCN event |
| Configure IGMP snooping policy | Configure the port filter rule |
| | Configure maximum items of port multicast group |
| | Configure the upper-limiting policy of port multicast group |
| Configure IGMP snooping proxy | Configure the IGMP snooping proxy |

### 2.2.1. Configure IGMP snooping Basic Functions

In the configuration tasks of IGMP snooping, you should first enable the IGMP snooping function so that the configuration of the other functions can take effect.

#### Configuration Condition

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

- Configure VLAN

### Enable IGMP snooping Function

After enabling IGMP snooping function, the device can run the IGMP snooping function.

Table 2-2 Enable IGMP snooping function

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable global IGMP snooping function | **ip igmp snooping** | Mandatory<br>By default, the global IGMP snooping function is not enabled. |
| Enable the IGMP snooping function of the specified VLAN | **ip igmp snooping vlan** *vlan-id* | Mandatory<br>By default, the IGMP snooping function is not enabled in the VLAN. |

**Note:**

- After enabling the global IGMP snooping function, you can enable the IGMP snooping function of the specified VLAN.

### Configure IGMP snooping Version

The configured IGMP snooping version and the processing rules of the IGMP protocol packets are as follows:

The configured IGMP snooping version is V3 and the device can process IGMP protocol packets of V1, V2 and V3;

The configured IGMP snooping version is V2 and the device can process the IGMP protocol packets of V1 and V2 and does not process V3 protocol packets, but make V3 protocol packets flood in VLAN.

The configured IGMP snooping version is V1 and the device can process the IGMP protocol packets of V1 and does not process V2 or V3 protocol packets, but make V2 and V3 protocol packets flood in VLAN.

Table 2-3 Configure IGMP snooping version

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure IGMP snooping version | **ip igmp snooping vlan** *vlan-id* **version** *version-number* | Optional<br>By default, the IGMP snooping version is 2. |

## 2.2.2. Configure IGMP snooping Querier

If there is no L3 multicast device in the network, it cannot realize the related functions of the IGMP querier. To solve the problem, you can configure the IGMP snooping querier on the L2 multicast device to realize the IGMP querier function so that L2 multicast device can set up and maintain multicast forwarding entry, so as to forward multicast service packets normally.

### Configuration Condition

Before configuring the basic functions of IGMP snooping querier, first complete the following task:

- Enable global and VLAN IGMP snooping function

### Enable IGMP snooping Querier

You should first enable the IGMP snooping querier function so that the configuration of the other features of the querier can take effect.

Table 2-4 Enable IGMP snooping querier

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable the IGMP snooping querier | **ip igmp snooping vlan** *vlan-id* **querier** | Mandatory<br>By default, the IGMP snooping querier of the specified VLAN is not enabled. |

### Configure Querier IP Address

The querier configured with IP address takes part in the election of the IGMP querier in VLAN and the querier fills the IP address in the source IP address field of the sent IGMP group query packet.

Table 2-5 Configure querier IP address

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the IP address of the querier | **ip igmp snooping vlan** *vlan-id* **querier address** *ip-address* | Mandatory<br>By default, the querier IP address of the specified VLAN is not configured. |

**Note:**

- When the querier IP address is not configured, the default source IP address of the querier is 0.0.0.0, but the querier does not send the IGMP group query packet with source IP address 0.0.0.0.

### Configure Query Interval of General Group

IGMP querier periodically sends the query packets of the general group to maintain the group member relation. You can modify the interval of sending the IGMP general group query packets according to the actuality of the network. For example, if the configured general group query interval is long, it can reduce the number of the IGMP protocol packets in the network, avoiding the network congestion.

Table 2-6 Configure query interval of general group

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure query interval of general group | **ip igmp snooping vlan** *vlan-id* **querier query-interval** *interval-value* | Optional<br>By default, the query interval of the general group is 125s. |

**Note:**

- In the same VLAN, the configured query interval of the general group should be larger than the maximum response time. Otherwise, the configuration cannot succeed.

### Configure Max. Response Time

The general group query packet sent by IGMPv2 querier contains the maximum response time field. The multicast receiver sends the member report packets within the maximum response interval.

Table 2-7 Configure the maximum response time

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the maximum response time | **ip igmp snooping vlan** *vlan-id* **querier max-response-time** *time-value* | Optional<br>By default, the maximum response time is 10s. |

**Note:**

- In one VLAN, the configured maximum response time should be smaller than the query interval of the general group. Otherwise, the configuration cannot succeed.

### Configure Query Interval of Specified Group

When the IGMP querier receives the leave packet of one multicast group, it sends the query packet of the specified group to query the segment for the multicast group, so as to know whether the subnet has the member of the multicast group. If not receiving the member report packet of the multicast group after waiting for “last life period”, delete the information of the multicast group.

Table 2-8 Configure query interval of specified group

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure query interval of specified group | **ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *interval-value* | Optional<br>By default, the query interval of the specified group is 1000 ms. |

### Configure Fast Leave

If the device receives the leave packet of one multicast group after configuring fast leave, the device does not send the query packet of the specified group to the port any more and the information of the multicast group is deleted at once.

Table 2-9 Configure fast leave

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the fast leave | **ip igmp snooping vlan** *vlan-id* **immediate-leave** | Mandatory<br>By default, the fast leave function of the specified VLAN is not enabled. |

**Note:**

- There are multiple receivers of the same multicast group in the device port at the same time. When the port receives the IGMP leave packet of the multicast group sent by one receiver and if fast leave is configured in the VLAN of the device port, the multicast services of the other receivers are interrupted.

## 2.2.3. Configure IGMP snooping Router Port

IGMP snooping router port is the port receiving IGMP group query packets or multicast routing protocol packets. When the device receives the IGMP member report or leave packet, forward the packet via IGMP snooping router port. In this way, the upper-connected router can maintain the IGMP member relation table correctly.

IGMP snooping router port can be dynamically learned or configured manually. IGMP snooping dynamic router port refreshes the age time by regularly receiving the IGMP group query packets or multicast routing protocol packets. IGMP snooping static router port does not age.

### Configuration Condition

Before configuring the IGMP snooping router port functions, first complete the following tasks:

- Enable global and VLAN IGMP snooping function
- Add port member in VLAN

### Configure IGMP snooping Static Router Port

After configuring IGMP snooping static router port, the device can forward the IGMP protocol packet via the port even the port does not receive the IGMP group query packet or multicast routing protocol packet. It can prevent the problem that the router port ages because the services of the upper-connected L3 multicast device are interrupted.

Table 2-10 Configure IGMP snooping static router port

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure IGMP snooping static router port | **ip igmp snooping vlan** *vlan-id* **mrouter** { **interface** *interface-name* \| **link-aggregation** *link-aggregation-id* } | Mandatory<br>By default, the IGMP snooping static router port is not configured. |

### Configure Age Time of IGMP snooping Dynamic Router Port

If the configured age time of the IGMP snooping dynamic router port is longer, it can prevent the problem that the router port of the upper-connected L3 multicast device is aged fast because of the service interruption.

Table 2-11 Configure age time of IGMP snooping dynamic router port

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure age time of IGMP snooping dynamic router port | **ip igmp snooping vlan** *vlan-id* **timer router-port expiry** *expiry-value* | Optional<br>By default, the age time of IGMP snooping dynamic router port is 255s. |

## 2.2.4. Configure IGMP snooping TCN Event

### Configuration Condition

Before configuring the IGMP snooping TCN event function, first complete the following task:

- Enable global and VLAN IGMP snooping function

### Enable fast convergence

When the network topology changes, generate the TCN event and the spanning tree root port actively sends the global IMGP leave packets (group address: 0.0.0.0) to request the IGMP querier to send the general group query packet, reaching the fast convergence.

After enabling IGMP snooping TCN event fast convergence, non-spanning tree root port also actively sends the global IGMP leave packet (group address: 0.0.0.0), reaching the fast convergence.

Table 2-12 Enable fast convergence

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable fast convergence | **ip igmp snooping tcn query solicit** | Mandatory<br>By default, the fast convergence is not enabled in the TCN event. |

### Configure Query Interval of TCN Event

When the TCN event happens, IGMP snooping querier sends the general group query according to the TCN event query interval.

Table 2-13 Configure query interval of TCN event

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the query interval of the TCN event | **ip igmp snooping vlan** *vlan-id* **querier tcn query interval** *interval-value* | Optional<br>By default, the query interval of the TCN event is 31s. |

### Configure Query Times of TCN Event

When the TCN event happens, IGMP snooping querier sends the general group query according to the query interval of the TCN event. After the sending times reaches the configured query times of the TCN event, restore to the query interval of the general group.

Table 2-14 Configure query times of TCN event

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the query times of the TCN event | **ip igmp snooping vlan** *vlan-id* **querier tcn query count** *count-number* | Optional<br>By default, the query times of the TCN event is 2. |

## 2.2.5. Configure IGMP snooping Policy

IGMP snooping policy is mainly used to control the receiver on the port, so as to control the multicast flow and limit the receiver action. In the setup L2 multicast flow forwarding environment, you also can apply the IGMP snooping policy.

### Configuration Condition

Before configuring the IGMP snooping policy, first complete the following task:

- Enable global and VLAN IGMP snooping function

### Configure Port Filter Rule

When the receiver hopes to get the multicast service, actively initiate the IGMP member report packet and the device judges according to the applied port filter rule in the port: refuse the user to add the destination multicast group; permit the user to add the destination multicast group; limit the times and time of the user adding the destination multicast group.

Table 2-15 Configure port filter rule

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter the IGMP profile configuration mode | **ip igmp profile** *profile-id* | - |
| Configure the range of the refused multicast group | **deny** { **all** \| *low-ip-address* [ *high-ip-address* ] } | Optional<br>By default, the range of the refused multicasts group is not configured. |
| Configure the range of the permitted multicast group | **permit** { **all** \| *low-ip-address* [ *high-ip-address* ] } | Optional<br>By default, the range of the permitted multicasts group is not configured. |

| Step | Command | Description |
|---|---|---|
| Configure the preview multicast group rule | **preview** { **all** \| *low-ip-address* [ *high-ip-address* ] \| **count** *count-number* \| **interval** *interval-time* \| **time** *time-duration* } | Optional<br>By default, the preview multicast group rule is not configured. |
| Return to global configuration mode | **exit** | - |
| Enter L2 Ethernet interface configuration mode | **interface** *interface-name* | You should select one of them.<br>After entering L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port; after entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group. |
| Enter aggregation group configuration mode | **link-aggregation** *link-aggregation-id* | |
| In the port, apply the IGMP port filter rule | **ip igmp filter** *profile-number* | Mandatory<br>By default, the IGMP port filter rule is not applied in the port. |

**Note:**

- Multicast group address can only be in one IGMP profile filter rule: deny, permit and preview. The new rule covers the old rule.
- Reset period of preview times > preview time × preview times + preview interval × (preview time – 1).

### Configure Maximum Number of Port Multicast Groups

The maximum number of the port multicast groups can limit the number of the multicast groups the receiver is added to.

Table 2-16 Maximum number of port multicast groups

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |

| Step | Command | Description |
|---|---|---|
| Enter L2 Ethernet interface configuration mode | **interface** *interface-name* | You should select one of them.<br>After entering L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port; after entering the aggregation group configuration mode, the subsequent configuration just takes effect on the aggregation group. |
| Enter aggregation group configuration mode | **link-aggregation** *link-aggregation-id* | |
| Configure maximum number of the multicast groups in the port | **ip igmp max-groups** *number* | Optional<br>By default, the maximum number of the multicast groups the port can dynamically be added to is 500. |

### Configure Upper-limitation Policy of Port Multicast Groups

When the number of the multicast groups the receiver is added to exceeds the configured maximum number of the multicast groups: If the upper-limitation policy of the port multicast group is replace, the new added multicast group on the device automatically replaces the existing multicast group; if the upper-limitation policy of the port multicast group is refuse, refuse the new added multicast group.

Table 2-17 Configure upper-limitation policy of port multicast group

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter L2 Ethernet interface configuration mode | **interface** *interface-name* | You should select one of them.<br>After entering L2 Ethernet interface configuration mode, the subsequent configuration just takes effect on the current port; after entering the aggregation group configuration mode, the subsequent configuration just |
| Enter aggregation group configuration mode | **link-aggregation** *link-aggregation-id* | |

| Step | Command | Description |
|---|---|---|
| | | takes effect on the aggregation group. |
| Configure the upper-limitation policy of the port multicast group | **ip igmp max-groups action** { **deny \| replace** } | Optional<br>By default, the processing action after the number of the multicast groups the port is dynamically added to reaches the maximum is refuse. |

### Configure the Interface to Control the PIM JOIN Packet

After configuring the interface to control the PIM JOIN packet, the JOIN packet is processed by the software, not by hardware.

Table 2-18 Configure controlling the PIM JOIN packet of the interface

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the interface to control the PIM JOIN packet | **ip igmp snooping vlan** *vlan-id* **ctrl-pim** | Mandatory<br>By default, do not control the PIM JOIN packet of the specified VLAN. |

**Note:**

- Before enabling the function, flood the JOIN packet in the VLAN. After enabling the function, the packet is sent to CPU, and does not flood in the VLAN.

## 2.2.6. Configure IGMP Snooping Proxy

When there are many receivers of the multicast group in the network, to reduce the number of the IGMP member report and leave packets received by the upstream multicast device and reduce the system cost effectively, you can configure IGMP snooping proxy on the device.

IGMP snooping proxy deputizes the downstream receiver to send the IGMP member report packets and leave packets to the upstream device and also can answer the IGMP group query packet sent by the upstream multicast device and then send the IGMP group query packet to the downstream device.

### Configuration Condition

Before configuring the IGMP snooping proxy function, first complete the following task:

- Enable global and VLAN IGMP snooping function

### Configure IGMP Snooping Proxy

Table 2-19 Configure IGMP snooping proxy

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure IGMP snooping proxy | **ip igmp snooping proxy vlan** *vlan-id* **upstream** { **interface** *interface-name* \| **link-aggregation** *link-aggregation-id* } | Mandatory<br>By default, IGMP agent port is not configured in VLAN. |

## 2.2.7. IGMP snooping Monitoring and Maintaining

Table 2-20 IGMP snooping monitoring and maintaining

| Command | Description |
|---|---|
| **clear ip igmp snooping groups** [ **grp-addr** *ip-address* \| **vlan** *vlan-id* [ **grp-addr** *ip-address-in-vlan* ] ] | Clear the IGMP snooping group information |
| **clear ip igmp snooping statistics vlan** *vlan-id* [ **interface** *interface-name* \| **link-aggregation** *link-aggregation-id* ] | Clear the IGMP protocol packet statistics information |
| **show ip igmp snooping proxy member database** [ **vlan** *vlan-id* ] | Display the IGMP snooping proxy member database information |
| **show ip igmp snooping proxy special query source-list** [ **vlan** *vlan-id* ] | Display the source list of the specified source query received by IGMP snooping proxy |
| **show ip igmp snooping proxy upstream** [ **vlan** *vlan-id* ] | Display the IGMP snooping proxy running information |
| **show ip igmp snooping debugging** | Display the IGMP snooping debugging status information |
| **show ip igmp snooping egress_table** | Display the L2 forwarding table of IGMP snooping |

| Command | Description |
|---|---|
| **show ip igmp snooping groups** [ **vlan** *vlan-id* ] [ **grp-addr** *ip-address* ] | Display the IGMP snooping multicast group information |
| **show ip igmp snooping groups** [ **vlan** *vlan-id* ] **count** | Display the number of IGMP snooping multicast groups |
| **show ip igmp snooping groups detail** [ **vlan** *vlan-id* ] [ **grp-addr** *ip-address* ] | Display the details of IGMP snooping multicast group |
| **show ip igmp snooping interface statistics** | Configure the statistics information of the multicast groups the IGMP snooping port is added to |
| **show ip igmp snooping l3_ip_table** | Display the L3 IP forwarding table of IGMP snooping |
| **show ip igmp snooping mcast_table** | Display the forwarding table of IGMP snooping |
| **show ip igmp snooping mrouter** [ **vlan** *vlan-id* ] | Display the IGMP snooping router port information |
| **show ip igmp snooping querier** [ **vlan** *vlan-id* ] | Display the IGMP snooping querier information |
| **show ip igmp snooping statistics vlan** *vlan-id* [ **interface** *interface-name* \| **link-aggregation** *link-aggregation-id* ] | Display the IGMP packet statistics information of the IGMP snooping port |
| **show ip igmp snooping** [ **vlan** *vlan-id* [ **info** ] ] | Display the IGMP snooping information |
| **show multicast control** [ **all-info \| interface** *interface-name* \| **link-aggregation** *link-aggregation-id* ] | Display the information of the L2 multicast control |

## 2.3. Typical Configuration Example of IGMP snooping

### 2.3.1. Configure IGMP snooping

#### Network Requirements

- Device1 configures the multicast route protocol; Device2 enables IGMP snooping; PC1 and PC2 are the receivers of the multicast service; PC3 is the receiver of the non-multicast service.
- Multicast Server sends the multicast service packets; PC1 and PC2 can receive the multicast service packets; PC3 cannot receive the multicast service packet.

#### Network Topology

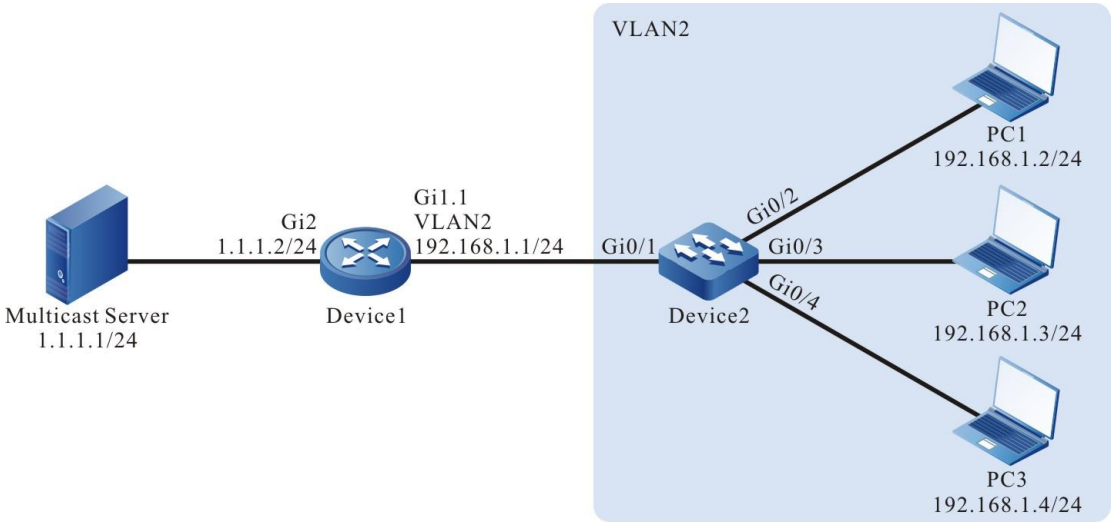


Figure 2-1 Network topology of IGMP snooping

#### Configuration Steps

**Step 1:** Device1 configure the interface IP address and enables the multicast route protocol. (omitted)

**Step 2:** Configure Device2.

#Create VLAN2 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#Configure the link type of the port gigabitethernet0/2-gigabitethernet0/4 on Device2 as Access, permitting the services of VLAN2 to pass.

```
Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/1 on Device2 as Trunk, permitting the services of VLAN2 to pass; PVID is configured as 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
```

```
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#Enable dropping unknown multicast in VLAN2.

```
Device2(config)#vlan 2
Device2(config-vlan2)#l3-multicast drop-unknown
Device2(config-vlan2)#exit
```

#Enable IGMP snooping.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
```

**Step 3:** Check the result.

# PC1 and PC2 send IGMPv2 member report packet to add multicast group 224.1.1.1.

#View the multicast member table of Device2.

```
Device2#show ip igmp snooping groups
VLAN ID  Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires Uptime
_______ ________________ _____________ _______ _____________    _________
2        gi0/2        224.1.1.1   00:03:26  192.168.1.2  stopped          00:00:55
2        gi0/3        224.1.1.1   00:03:44  192.168.1.3  stopped          00:00:40
```

#Multicast Server sends the multicast service packet with destination address 224.1.1.1; PC1 and PC2 can correctly receive the multicast service packet; PC3 cannot receive the multicast service packet.

## 2.3.2. Configure Multicast Receiving Control

### Network Requirements

- Device1 configures multicast routing protocol.
- Device2 enables IGMP snooping, configures multicast receiving control and applies to the corresponding port.
- Multicast Server sends the multicast service packet; PC1 and PC2 can receive the multicast service packet.

## Network Topology

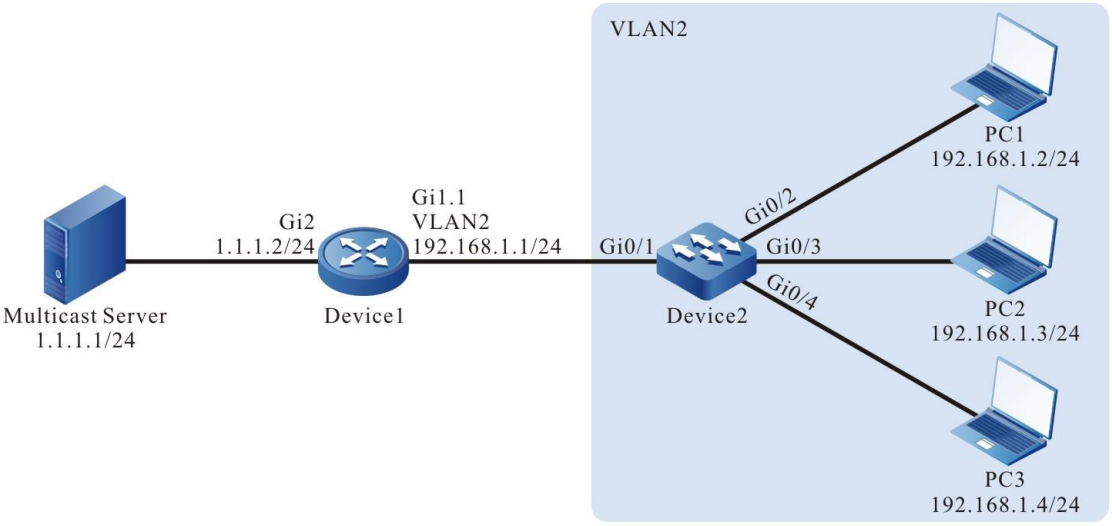


Figure 2-2 Network topology of configuring multicast receiving control

## Configuration Steps

**Step 1:** Device1 configures the interface IP address and enables the multicast route protocol. (omitted)

**Step 2:** Configure Device2.

#Create VLAN2 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#Configure the link type of the port gigabitethernet0/2-gigabitethernet0/4 on Device2 as Access, permitting the services of VLAN2 to pass.

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/1 on Device2 as Trunk, permitting the services of VLAN2 to pass; PVID is configured as 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#Enable IGMP snooping.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
```

#Configure multicast receiving control policy profile1, permits to add multicast group 224.1.1.1 and apply to port gigabitethernet0/2.

```
Device2(config)#ip igmp profile 1
Device2(config-igmp-profile)#permit 224.1.1.1
Device2(config-igmp-profile)#exit
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#ip igmp filter 1
Device2(config-if-gigabitethernet0/2)#exit
```

#Configure multicast receiving control policy profile2, preview multicast group 224.1.1.1 and apply to port gigabitethernet0/3.

```
Device2(config)#ip igmp profile 2
Device2(config-igmp-profile)#preview 224.1.1.1
Device2(config-igmp-profile)#exit
Device2(config)#interface gigabitethernet 0/3
Device2(config-if-gigabitethernet0/3)#ip igmp filter 2
Device2(config-if-gigabitethernet0/3)#exit
```

#Configure multicast receiving control policy profile3, refuse adding to multicast group 224.1.1.1 and apply to port gigabitethernet0/4.

```
Device2(config)#ip igmp profile 3
Device2(config-igmp-profile)#permit all
Device2(config-igmp-profile)#deny 224.1.1.1
Device2(config-igmp-profile)#exit
Device2(config)#interface gigabitethernet 0/4
Device2(config-if-gigabitethernet0/4)#ip igmp filter 3
Device2(config-if-gigabitethernet0/4)#exit
```

**Step 3:** Check the result.

#PC1, PC2 and PC3 send IGMPv2 member report packet to add to multicast group 224.1.1.1.

#View multicast member table of Device2.

```
Device2#show ip igmp snooping groups
IGMP Snooping Group Membership
Total 2 groups

VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires
Uptime
```

---

2 gi0/2 224.1.1.1 00:04:19 192.168.1.2 stopped 00:00:01

2 gi0/3 224.1.1.1 00:04:19 192.168.1.3 stopped 00:00:01

PC1 and PC2 can add to multicast group 224.1.1.1; PC3 does not add to multicast group 224.1.1.1.

# Multicast Server sends the multicast service packet with destination address 224.1.1.1.

PC1 and PC2 can correctly receive the multicast service packet; PC3 cannot receive the multicast service packet.

#After waiting for 10s, view the multicast member table of Device2 and multicast receiving control information of gigabitethernet0/3.

Device2#show ip igmp snooping groups

IGMP Snooping Group Membership

Total1 group

VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires Uptime

---

2 gi0/2 224.1.1.1 00:04:10 192.168.1.2 stopped 00:00:10

Device2#show multicast control interface gigabitethernet 0/3

ip multicast control gigabitethernet0/3 vlan 2 information

---

profile: 2

group right information:

preview: 224.1.1.1

preview information:

preview count: 3

preview count remain: 2

preview time: 10 (s)

preview interval: 60 (s)

group information:

group: 224.1.1.1

uptime: 00:00:10

next preview time remain: 00:00:60

After the preview time of port gigabitethernet0/3 arrives (after 10s), the group member entry is deleted; PC1 can correctly receive the multicast service packet; PC2 and PC2 cannot receive the multicast service packet.

## 2.3.3. Configure IGMP Snooping Proxy

### Network Requirements

- Device1 configures multicast routing protocol.
- Device2 enables IGMP snooping and GMP snooping proxy.
- Multicast Server sends the multicast service packet; PC1, PC2, and PC3 can correctly receive the multicast service packet.

### Network Topology

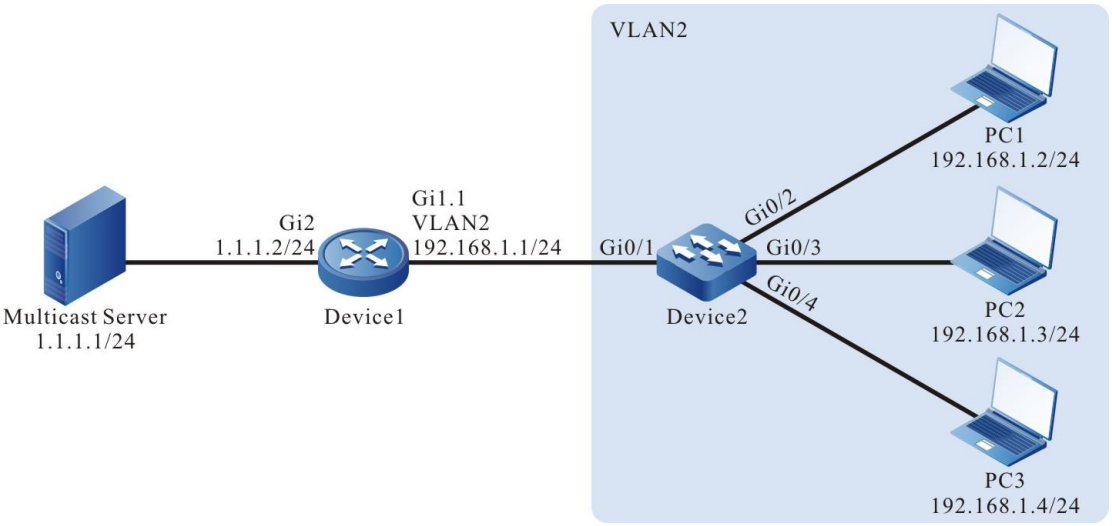


Figure 2-3 Network topology of configuring IGMP snooping proxy

### Configuration Steps

**Step 1:** Device1 configures the interface IP address and enables the multicast route protocol.

```
Device1#configure terminal
Device1(config)#ip multicast-routing
Device1(config)#interface gigabitethernet1.1
Device1(config-if-gigabitethernet1.1)# ip address 192.168.1.1 255.255.255.0
Device1(config-if-gigabitethernet1.1)# encapsulation dot1q 2
Device1(config-if-gigabitethernet1.1)# ip pim sparse-mode
Device1(config-if-gigabitethernet1.1)# exit
Device1(config)#interface gigabitethernet2
Device1(config-if-gigabitethernet2)# ip address 1.1.1.2 255.255.255.0
Device1(config-if-gigabitethernet2)# ip pim sparse-mode
Device1(config-if-gigabitethernet2)# exit
```

**Step 2:** Configure Device2.

#Create VLAN2 on Device2.

```
Device2#configure terminal
Device2(config)#vlan 2
```

```
Device2(config-vlan2)#exit
```

#Configure the link type of the port gigabitethernet0/2-gigabitethernet0/4 on Device2 as Access, permitting the services of VLAN2 to pass.

```
Device2(config)#interface gigabitethernet 0/2-0/4
Device2(config-if-range)#switchport access vlan 2
Device2(config-if-range)#exit
```

#Configure the link type of port gigabitethernet0/1 on Device2 as Trunk, permitting the services of VLAN2 to pass; PVID is configured as 1.

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device2(config-if-gigabitethernet0/1)#switchport trunk pvid vlan 1
Device2(config-if-gigabitethernet0/1)#exit
```

#Enable IGMP snooping in VLAN2; configure IGMP snooping querier address as 192.168.1.254.

```
Device2(config)#ip igmp snooping
Device2(config)#ip igmp snooping vlan 2
Device2(config)#ip igmp snooping vlan 2 querier
Device2(config)#ip igmp snooping vlan 2 querier address 192.168.1.254
```

#Configure IGMP snooping proxy.

```
Device2(config)#ip igmp snooping proxy vlan 2 upstream interface gigabitethernet 0/1
Device2(config)#exit
```

**Step 3:** Check the result.

#PC1, PC2 and PC3 successively sends IGMPv2 member report packets to add to multicast group 224.1.1.1.

#View the IGMP snooping proxy information of Device2.

```
Device2#show ip igmp snooping proxy upstream vlan 2
vlan 2 proxy upstream information:
------------------------------
upstream interface                : gi0/1
upstream querier compatmode version    : 2
upstream querier address          : 192.168.1.1
upstream report source address          : 192.168.1.4upstream querier query interval      : 125s
upstream querier query response interval: 10s
upstream querier LMQI             : 1s
upstream querier LMQC             : 2
```

```
upstream querier robustness variable    : 2
upstream querier present timer          : 00:02:50
upstream V1 querier present timer       : stopped
upstream V2 querier present timer       : 00:02:55
```

#View multicast member table of Device2 and IGMP snooping proxy member database.

```
Device2#show ip igmp snooping groups
IGMP Snooping Group Membership
Total 3 groups

VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires
Uptime
_____________________________________________________
_____________________________
2       gi0/2         224.1.1.1     00:04:09  192.168.1.2 stopped          00:00:14
2       gi0/3         224.1.1.1     00:04:09  192.168.1.3 stopped          00:00:11
2       gi0/4         224.1.1.1     00:04:12  192.168.1.4 stopped          00:00:07
You can see that PC1, PC2 and PC3 add to multicast group 224.1.1.1.
Device2#show ip igmp snooping proxy member database vlan 2
IGMP Snooping Proxy Member Database Table
Total 1 group

VLAN ID  Group Address    Mode    Source Address
-------  ---------------  -------  ---------------
2        224.1.1.1        EXCLUDE  *
```

#View multicast member table of Device1.

```
Device1#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address    Interface          Uptime   Expires  Last Reporter   V1 Expires    V2
Expires
224.1.1.1        gigabitethernet1.1     00:00:15 00:04:11 192.168.1.2       stopped
```

You can see that when PC adds to multicast group 224.1.1.1, Device2 can only forward the first IGMPv2 member report packet to Device1 and the other are all dropped.

#Multicast Server sends the multicast service packet with destination address 224.1.1.1; PC1, PC2 and PC3 can correctly receive the multicast service packet.

#PC1 and PC2 send IGMPv2 leave packet to leave multicast group 224.1.1.1.

```
Device2#show ip igmp snooping groups
IGMP Snooping Group Membership
```

```
Total 1 group

VLAN ID Interface Name Group Address Expires Last Reporter V1 Expires V2 Expires
Uptime
-------------------------------------------------------------------------------
--
2       gi0/4         224.1.1.1     00:03:54 192.168.1.4  stopped          00:06:37
Device1#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address    Interface          Uptime   Expires  Last Reporter   V1 Expires   V2
Expires
224.1.1.1        gigabitethernet1.1 00:06:48 00:03:48 192.168.1.2     stopped
```

After PC1 and PC2 leave multicast group 224.1.1.1, PC3 does not leave the multicast group, so there is still group member PC3 in the multicast member table. Therefore, Device2 does not send the leave packet of the multicast group to Device1.

#PC3 sends the IGMPv2 leave packet to leave multicast group 224.1.1.1; view multicast member table of Device2 and Device1.

```
Device2#show ip igmp snooping groups
```

You can see that there is no multicast member table on Device2.

```
Device1#show ip igmp groups
```

There is no multicast member on Device1. When the last group member PC3 leaves the multicast group, Device2 sends the leave packet of the multicast group to Device1.

#PC1, PC2 and PC3 cannot receive the multicast service packet.

# 3. IPV4 MULTICAST BASICS

## 3.1. Overview

IPv4 multicast basics is the basis of running the IP multicast protocol and the common part of all multicast protocols. No matter which multicast route protocol runs, we first need to enable the IP multicast forwarding function so that the device can forward the multicast service packets.

## 3.2. Basic Function Configuration of IPv4 Multicast

Table 3-1 Basic function configuration list of IPv4 multicast

| Configuration Task | |
|---|---|
| Enable IP multicast forwarding | Enable the IP multicast forwarding |
| Configure IP multicast forwarding rule | Configure the multicast forwarding management edge |
| | Configure the regular detection of the multicast forwarding |
| | Configure the multicast route table limitation |
| | Configure the multicast interface TTL threshold |

### 3.2.1. Enable IP Multicast Forwarding

IP multicast forwarding is the basic module of the multicast forwarding. The device can forward the IP multicast service packets only after enabling the IP multicast forwarding function. Both the general IP multicast forwarding and IP multicast fast forwarding are controlled by whether to enable the IP multicast forwarding.

IP multicast fast forwarding is one IPv4 fast multicast forwarding technology designed to improve the forwarding performance of the service packets. It completes the route selection and service processing for a time, so as to reduce the resource consumption caused by the switching between the internal tasks of the system and the packet cache management. At last, improve the data forwarding performance of the whole system.

#### Configuration Condition

Before configuring the IP multicast forwarding function, first complete the following task:

- Configure the IP address of the interface, making the neighboring node network layer reachable;
- Configure any unicast routing protocol, making the routes in the domain reachable;
- Configure any multicast routing protocol.

### Enable IP Multicast Forwarding

The device can forward the IP multicast service packets only after enabling the IP multicast forwarding function.

Table 3-2 Enable IP multicast forwarding

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Enable IP multicast forwarding | **ip multicast-routing** [ **vrf** *vrf-name* ] | Mandatory<br>By default, the IP multicast forwarding is not enabled. |

## 3.2.2. Configure IP Multicast Forwarding Rule

### Configuration Condition

Before configuring the IP multicast forwarding rule, first complete the following task:

- Configure interface IP address, making the neighboring node network layer reachable;
- Configure any unicast routing protocol, making the routes in the domain reachable;
- Enable IP multicast forwarding;
- Configure any multicast route protocol.

### Configure Multicast Forwarding Management Edge

The multicast forwarding management edge mainly realizes the filtering for the multicast packets. After configuring the management edge, the device can filter the multicast service packets and only the multicast service permitted by ACL can pass.

Table 3-3 Configure multicast forwarding management edge

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure multicast forwarding management edge | **ip multicast boundary**<br>{ *access-list-number* \| *access-list-name* } | Mandatory<br>By default, the multicast forwarding management edge is not configured. |

### Configure Regular Detection of Multicast Forwarding

After configuring the regular detection of the multicast forwarding and if the number of the specified forwarded multicast service packets in the unit time is smaller than the configured minimum number, print the alarm information.

Table 3-4 Configure the regular detection of the multicast forwarding

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Configure the regular detection of the multicast forwarding | **ip multicast heartbeat** *group-ip-address source-ip-address minmum-packets interval-value* [ **vrf** *vrf-name* ] | Mandatory<br>By default, do not perform the regular detection of the multicast forwarding. |

### Configure Multicast Route Table Limitation

Configure the maximum quantity limitation of the multicast route table. After exceeding the maximum quantity limitation of the multicast route table, do not create new multicast route table any more.

Table 3-5 Configure the multicast route table limitation

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Configure the multicast route table limitation | **ip multicast route-limit** *number-value* [ **vrf** *vrf-name* ] | Optional<br>By default, the maximum number of the multicast route table is 8192. |

### Configure TTL Threshold of Multicast Interface

After configuring the TTL threshold of the multicast ingress interface, only the multicast service packet whose TTL is larger than the threshold can be accepted, while the multicast packet whose TTL is smaller than or equal to the threshold is dropped.

After configuring the TTL threshold of the multicast egress interface, only the multicast service packet whose TTL minus 1 is still larger than the threshold can be forwarded, while the multicast packet whose TTL is smaller than or equal to the threshold is dropped.

Table 3-6 Configure the TTL threshold of the multicast interface

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Configure the TTL threshold of the multicast ingress interface | **ip multicast in-threshold** *number-value* | Optional<br>By default, the TTL threshold of the multicast ingress interface is 0. |
| Configure the TTL threshold of the multicast egress interface | **ip multicast out-threshold** *number-value* | Optional<br>By default, the TTL threshold of the multicast egress interface is 0. |

### 3.2.3. Monitoring and Maintaining of IPv4 Multicast Basics

Table 3-7 Monitoring and maintaining of IPv4 multicast basics

| Command | Description |
|---|---|
| **clear ip mcache** [ **source** *source-ip-address* ] [ **group** *group-ip-address* ] [ **all \| vrf** *vrf-name* ] | Clear the multicast route entry |
| **show ip mcache** [ **source** *source-ip-address* ] [ **group** *group-ip-address* ] [ **vrf** *vrf-name* ] | Display the multicast route table information |
| **show ip mvif** [ **vrf** *vrf-name* ] | Display the multicast virtual interface information |

# 4. IGMP

## 4.1. Overview

IGMP (Internet Group Management Protocol) is the protocol for managing the IP multicast members in the TCP/IP protocol stack, used to set up and maintain the multicast group member relation between the IP host and the direct neighboring multicast device.

IGMP has three versions. Currently, the widely-used is IGMPv2. IGMPv2 has three kinds of packets: query packet, group member relation report packet, and group member leave packet.

Query packet includes the general query packet and the specified group query packet. The device gets to know which members there are in the direct-connected network via the general query packets and whether there are the members of one specified group in the direct-connected network via the specified group query packets.

Group member relation report: When the host wants to add into one multicast group, the host immediately sends the group member relation report to the desired multicast group. When the host receives one query packet, it also sends the group member relation report.

Group member leave packet: When the host leaves one multicast group, send one group member leave report. When the device receives the group member leave packet, send the specified group query to confirm whether one specified group has members.

## 4.2. IGMP Function Configuration

Table 4-1 IGMP function configuration list

| **Configuration Task** | |
|---|---|
| Configure IGMP basic functions | Enable the IGMP protocol |
| | Configure the IGMP version |
| | Configure static group adding |
| | Configure multicast group filter |
| | Configure SSM multicast group filter |
| Adjust and optimize the IGMP network | Configure the query interval of the general group |
| | Configure the robustness factor |
| | Configure the maximum response time |
| | Configure the specified group query |

| Configuration Task | |
|---|---|
| | Configure the other querier timeout |
| | Configure the fast leave |
| Configure the IGMP SSM mapping | Configure the IGMP SSM mapping |

### 4.2.1. Configure IGMP Basic Functions

#### Configuration Condition

Before configuring the IGMP basic functions, first complete the following task:

- Configure the interface network layer address, making the neighboring node network layer reachable

#### Enable IGMP Protocol

Table 4-2 Enable the IGMP protocol

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable the IP multicast forwarding | **ip multicast-routing** | Mandatory<br>By default, the IP multicast forwarding is disabled. |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Enable the IGMP protocol | **ip pim sparse-mode** | Mandatory<br>By default, IGMP is disabled.<br>When the interface enables the multicast route protocol, automatically enable IGMP. Only after enabling IGMP, all IGMP configurations can take effect. |

### Configure IGMP Version

Table 4-3 Configure the IGMP version

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the IGMP version | **ip igmp version** *version-number* | Mandatory<br>By default, the IGMP version is 2. |

**Note:**

- Because the packet structure and kind of different versions of IGMP protocols are different, it is suggested to configure the same version of IGMP for all devices on the same subnet.

### Configure Static Group Adding

After configuring one static group or source group in the interface, the device regards that the interface has the receiver of the multicast group or source group.

Table 4-4 Configure static group adding

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the static group adding | **ip igmp static-group** *group-ip-address* [ *source-ip-address* ] | Mandatory<br>By default, the interface is not added to any multicast group or source group in the static mode. |

### Configure Multicast Group Filter

The interface configured with the IGMP multicast group filter filters the group member relation report in the segment according to the ACL rules and only the group member relation report permitted by ACL is processed and the un-permitted is directly dropped. For the existing but not permitted by ACL multicast group, immediately delete the multicast group information.

Table 4-5 Configure multicast group filter

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the IGMP multicast group filter | **ip igmp access-group** { *access-list-number* \| *access-list-name* } | Mandatory<br>By default, the multicast group filter is not configured. |

**Note:**

- **ip igmp access-group** Command only supports the standard ACL.

### Configure SSM Multicast Group Filter

After configuring the range of the source groups received by IGMP, filter the received source group member relation report to limit the source group range the interface serves. For the groups belonging to the PIM-SSM range, only the IGMPv3 non (IS_EX, TO_EX) member relation report permitted by the access list (S, G ) can be accepted.

Table 4-6 Configure the SSM multicast group filter

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the SSM multicast group filter | **ip igmp ssm-access-group** { *access-list-number* \| *access-list-name* } | Mandatory<br>By default, do not filter to limit the SSM group members. |

**Note:**

- **ip igmp ssm-access-group** can take effect only when the interface enables IGMPv3.
- **ip igmp ssm-access-group** takes effect only for the source groups in the PIM SSM range.
- **ip igmp ssm-access-group** only supports the extended ACL.

## 4.2.2. Adjust and Optimize IGMP Network

### Configuration Condition

Before adjusting and optimizing the IGMP network, first complete the following task:

- Configure interface network layer address, making the neighboring node network layer reachable
- Enable the IGMP protocol

### Configure Query Interval of General Group

IGMP querier periodically sends the general group query packets to maintain the group member relation. You can modify the interval of sending the IGMP general group query packets according to the actuality of the network.

Table 4-7 Configure the query interval of the general group

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the query interval of the general group | **ip igmp query-interval** *interval-value* | Optional<br>By default, the interval of sending the IGMP general group query packets is 125s. |

**Note:**

- The genera query intervals of the devices on the same segment should try to keep consistent.
- The general group query interval should be larger than the maximum response time. Otherwise, the configuration cannot succeed.

### Configure Robustness Factor

Table 4-8 Configure robustness factor

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the robustness factor | **ip igmp robustness-variable** *variable-value* | Optional<br>By default, the robustness factor of the IGMP querier is 2. |

**Note:**

- After configuring the robustness factor, the following parameters also change with the robustness parameters:
- Group member timeout = Robustness factor * general group query time + maximum response time;
- Other querier timeout = Robustness factor * general group query time + maximum response time/2;
- The larger the robustness factor, the larger the IGMP group member timeout and other querier timeout. The user sets the value according to the actuality of the network.

### Configure Maximum Response Time

The general group query packet sent by the IGMPv2 querier contains the maximum response time field and the receiver sends the group member relation report within the maximum response interval. If the receiver does not send the group member relation report within the maximum response time, the device regards that the subnet does not have the receiver of the multicast group and deletes the multicast group information immediately.

Table 4-9 Configure the maximum response time

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the maximum response time | **ip igmp query-max-response-time** *seconds* | Optional<br>By default, the maximum response time of the IGMP general group query is 10s. |

### Configure Specified Group Query

After the IGMP querier receives the leave packet of one multicast group, send the specified group query packet to query the multicast group on the segment for “Specified group query times”. This is to know whether the subnet has the members of the multicast group. If not receiving the member relation report of the multicast group after waiting for “maximum response time”, delete the information of the multicast group.

Table 4-10 Configure the specified group query

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the query interval of the specified group | **ip igmp last-member-query-interval** *interval-value* | Optional<br>By default, the interval of sending the specified group query packets is 1s. |
| Configure the query times of the specified group | **ip igmp last-member-query-count** *count-value* | Optional<br>By default, the times of sending the specified group query packets is 2. |

**Note:**

- **ip igmp last-member-query-interval** and **ip igmp last-member-query-count** are invalid in IGMPv1, because the IGMPv1 host does not send leave packets when leaving one multicast group.

### Configure Other Querier Timeout

The device with the smallest address in one subnet is elected as the querier and the other devices are called non-querier. On the non-queriers, set one timeout as the timer of “other querier timeout” (the other queriers have timer) for the querier. When the non-querier receives the query packet of the querier, refresh the timer. When the timer times out, it indicates that the current IGMP querier becomes invalid and you need to re-elect the querier.

Table 4-11 Configure the other querier timeout

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the other querier timeout | **ip igmp query-timeout** *seconds* | Optional<br>By default, the other querier timeout is 255s. |

**Caution:**

- If the configure other querier timeout is smaller than the query interval, the querier in the network may change repeatedly.

### Configure Fast Leave

The end segment in the network only connects to one host, which performs the switching action of the multicast group frequently. To reduce the leave delay, you can configure the fast leave of the multicast group on the device.

After configuring the fast leave, the device receives the leave packet of one multicast group and checks whether the multicast group belongs to the fast leave range. If yes, the device does not send the specified group query packet to the segment any more and deletes the information of the multicast group immediately.

Table 4-12 Configure the fast leave

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the multicast group range of the fast leave | **ip igmp immediate-leave group-list** { *access-list-number* \| *access-list-name* } | Mandatory<br>By default, do not permit the fast leave of the multicast group, applicable to IGMPv2. |
| Configure the source group range of the fast leave | **ip igmp sg-immediate-leave sg-list** { *access-list-number* \| *access-list-name* } | Mandatory<br>By default, do not permit the fast leave of the source group, applicable to IGMPv3. |

### 4.2.3. Configure IGMP SSM Mapping

#### Configuration Conditions

Before configuring the IGMP SSM mapping, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable;
- Enable the IGMP protocol.

#### Configure IGMP SSM Mapping

To provide the PIM-SSM service for the receiver not supporting IGMPv3 in the PIM-SSM network, we can configure the IGMP SSM Mapping function on the device.

The user can configure the IGMP SSM Mapping rule according to the demand of the network receiver. The group member relation report permitted by the rule is converted to the IGMPv3 non-member (IS_EX, TO_EX) relation report, and the multicast source address is the source address specified by the IGMP SSM mapping rule.

Table 4-13 Configure the IGMP SSM mapping

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Enable the IGMP SSM Mapping | **ip igmp ssm-map enable** [ **vrf** *vrf-name* ] | Mandatory<br>By default, do not enable the IGMP SSM Mapping. |
| Configure the IGMP SSM Mapping rule | **ip igmp ssm-map static** { *access-list-number* **\|** *access-list-name* } *source-ip-address* [ **vrf** *vrf-name* ] | Mandatory<br>By default, there is no IGMP SSM Mapping rule. |

**Note:**

- The **ip igmp ssm-map static** command only supports the standard ACL.

## 4.2.4. Configure IGMP Proxy

### Configuration Conditions

Before configuring the IGMP proxy, first complete the following task:

- Configure the network layer address of the interface, making the neighboring node network layer reachable;
- Enable the IGMP protocol.

### Configure IGMP Proxy

IGMP proxy is an extension of the existing IGMP functions. IGMP proxy function refers to configuring one interface of the device as the upstream interface of IGMP proxy, and the other interfaces become the downstream interface of IGMP proxy. The IGMP proxy upstream interface acts as the IGMP host. The IGMP proxy will integrate the IGMP members learned by the downstream interface into the IGMP proxy member database, and the upstream interface of the IGMP proxy will send the IGMP report to the upstream IGMP inquirer according to the member status in the proxy member database.

Table 4-14 Configure the IGMP proxy

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Configure the IGMP proxy | **ip igmp proxying** | Mandatory<br>By default, do not enable the IGMP proxy. |

### 4.2.5. IGMP Monitoring and Maintaining

Table 4-15 IGMP monitoring and maintaining

| Command | Description |
|---|---|
| **clear ip igmpstat** | Clear the statistics information of the IGMP protocol packets |
| **clear ip igmp group** [ *group-ip-address* ] [ *interface-name* ] [ **vrf** *vrf-name* ] | Clear the IGMP multicast group information |
| **clear ip igmp proxy statistic** [ **vrf** *vrf-name* ] | Clear the IGMP proxy statistics information |
| **clear ip igmp statistic interface** *interface-name* [ **vrf** *vrf-name* ] | Clear the IGMP packet statistics information on the interface |
| **show ip igmp groups** [ [ **static** ] \| [ *interface-name* ] [ *group-ip-address* ] [ **detail** ] ] [ **vrf** *vrf-name* ] | Display the IGMP multicast group information |
| **show ip igmp interface** [ *interface-name* ] [ **vrf** *vrf-name* ] | Display the interface IGMP information |
| **show ip igmp proxy** { **group \| statistic** } [ **vrf** *vrf-name* ] | Display the IGMP proxy information |
| **show ip igmp ssm-map** [ **vrf** *vrf-name* ] | Display the IGMP SSM Mapping information |

| Command | Description |
|---|---|
| **show ip igmp statistic interface** *interface-name* [ **vrf** *vrf-name* ] | Display the statistics information of the IGMP packets |

## 4.3. IGMP Typical Configuration Example

### 4.3.1. Configure IGMP Basic Functions

#### Network Requirements

- The whole network runs the PIM-SM protocol.
- Device1, Device2, and Receiver are in the same LAN and Device2 is the querier.
- Receiver is one receiver of Device1 and Device2 end network.
- Run IGMPv2 between Device1, Device2 and end network.

#### Network Topology

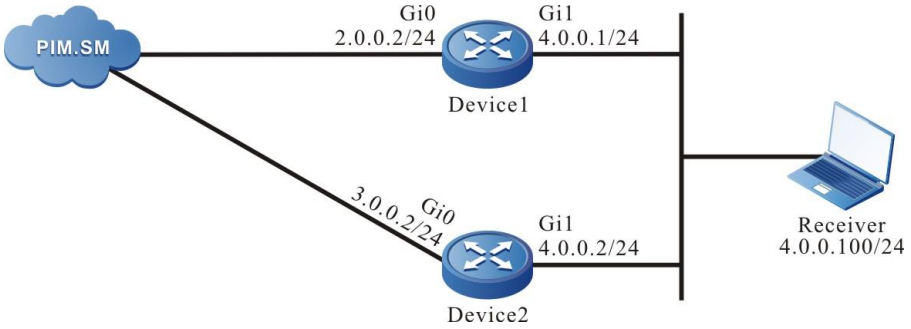


Figure 4-1 Networking of configuring IGMP basic functions

#### Configuration Steps

**Step 1:** Configure the IP address of the interface. (omitted)

**Step 2:** Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

#Configure Device1.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related interfaces.

```
Device1(config)#configure terminal
Device1(config)#ip multicast-routing
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip pim sparse-mode
Device1(config-if-gigabitethernet0)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#ip pim sparse-mode
Device1(config-if-gigabitethernet1)#exit
```

#Configure Device2.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related interfaces.

```
Device2(config)#configure terminal
Device2(config)#ip multicast-routing
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ip pim sparse-mode
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ip pim sparse-mode
Device2(config-if-gigabitethernet1)#exit
```

**Step3:** Check the result.

#View the IGMP version information and querier election result of Device2 interface gigabitethernet1.

```
Device2#show ip igmp interface gigabitethernet 1
Interface gigabitethernet1 (Index 50331921)
 IGMP Active, Querier (4.0.0.1)
 Default version 2
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 4.0.0.1
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1 seconds
 Last member query count is 2
 Group Membership interval is 260 seconds
 IGMP robustness variable is 2
```

#View the IGMP version information and querier election result of Device1 interface gigabitethernet1.

```
Device1#show ip igmp interface gigabitethernet 1
Interface gigabitethernet 1  (Index 50331921)
 IGMP Active, Non-Querier (4.0.0.1, Expires: 00:02:15)
 Default version 2
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 4.0.0.2
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
```

```
IGMP max query response time is 10 seconds configged, and 10 seconds is adopted
Last member query response interval is 1 seconds
Last member query count is 2
Group Membership interval is 260 seconds
IGMP robustness variable is 2
```

#Receiver sends the IGMPv2 member relation report to add to multicast group 225.1.1.1.

#Query the multicast member table of Device1.

```
Device1#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address   Interface        Uptime    Expires   Last Reporter   V1 Expires
225.1.1.1       gigabitethernet1 00:21:02  00:03:47  4.0.0.100       stopped
```

#Query the multicast member table of Device2.

```
Device2#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address   Interface        Uptime    Expires   Last Reporter   V1 Expires
225.1.1.1       gigabitethernet1 00:21:02  00:03:47  4.0.0.100       stopped
```

**Note:**

- After configuring the multicast protocol on the interface, automatically enable the IGMP function and run the IGMPv2 by default. You can configure the running IGMP version of the interface via the command ip igmp version.
- When multiple devices run IGMP in one LAN, elect the IGMP querier and the one with the smallest address is elected as the IGMP querier of the LAN.

## 4.3.2. Configure IGMP Static Adding

### Network Requirements

- The whole network runs the PIM-SM protocol.
- Receiver is one receiver of the Device end network.
- Run IGMPv2 between Device and the end network.
- Device interface gigabitethernet1 adds to multicast group 225.1.1.1 statically.

### Network Topology

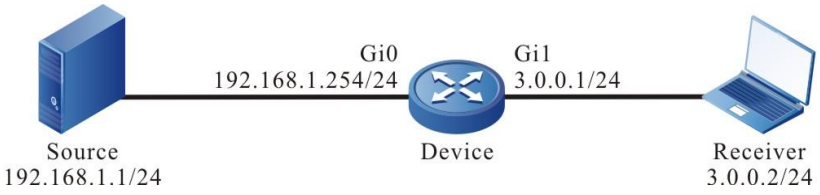


Figure 4-2 Networking of configuring IGMP static adding

## Configuration Steps

**Step 1:** Configure the IP address of the interface. (omitted)

**Step 2:** Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

#Configure Device.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related interfaces.

```
Device(config)#configure terminal
Device(config)#ip multicast-routing
Device(config)#interface gigabitethernet0
Device(config-if-gigabitethernet0)#ip pim sparse-mode
Device(config-if-gigabitethernet0)#exit
Device(config)#interface gigabitethernet1
Device(config-if-gigabitethernet1)#ip pim sparse-mode
Device(config-if-gigabitethernet1)#exit
```

#View the IGMP information of Device interface gigabitethernet1.

```
Device#show ip igmp interface gigabitethernet 1
Interface gigabitethernet1 (Index 50331921)
 IGMP Active, Querier (3.0.0.1)
 Default version 2
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 3.0.0.1
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1 seconds
 Last member query count is 2
 Group Membership interval is 260 seconds
 IGMP robustness variable is 2
```

**Step 3:** Device interface gigabitethernet 1 adds to multicast group 225.1.1.1 statically.

#Configure Device.

Device interface gigabitethernet 1 adds to multicast group 225.1.1.1 statically.

```
Device(config)#interface gigabitethernet1
Device(config-if-gigabitethernet1)#ip igmp static-group 225.1.1.1
Device(config-if-gigabitethernet1)#exit
```

**Step 4:** Check the result.

#Source sends the multicast packet with multicast group 225.1.1.1.

#View the multicast member table of Device.

```
Device#show ip igmp groups
IGMP Static Group Membership
Total 1 static groups
Group Address   Source Address   Interface
225.1.1.1       0.0.0.0         gigabitethernet1
```

#View the multicast route table of Device.

```
Device#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(*, 225.1.1.1)
Up time: 00:08:12
RP: 0.0.0.0
RPF nbr: 0.0.0.0
RPF idx: None
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
  gigabitethernet1
 Joined interface list:
 Asserted interface list:


(192.168.1.1, 225.1.1.1)
```

```
Up time: 00:07:24
KAT time: 00:02:22
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: TRUE
Flags:
  JOIN DESIRED
  COULD REGISTER
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    register_vif0
  Asserted interface list:
  Outgoing interface list:
    register_vif0
    gigabitethernet1
  Packet count 8646421

(192.168.1.1, 225.1.1.1, rpt)
Up time: 00:07:24
RP: 0.0.0.0
Flags:
  RPT JOIN DESIRED
  RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    gigabitethernet1
```

#Receiver can receive the multicast packet with multicast group 225.1.1.1 sent by Source.

### 4.3.3. Configure IGMP SSM Mapping

#### Network Requirements

- The whole network runs the PIM-SM protocol.
- Receiver1, Receiver2, Receiver3, and Device2 are all in one LAN.
- Run IGMPv3 between Device2 and the end network.
- Use the IGMP SSM mapping on Device2 so that Receiver2 and Receiver3 can only receive the multicast service packets sent by Source1.

## Network Topology

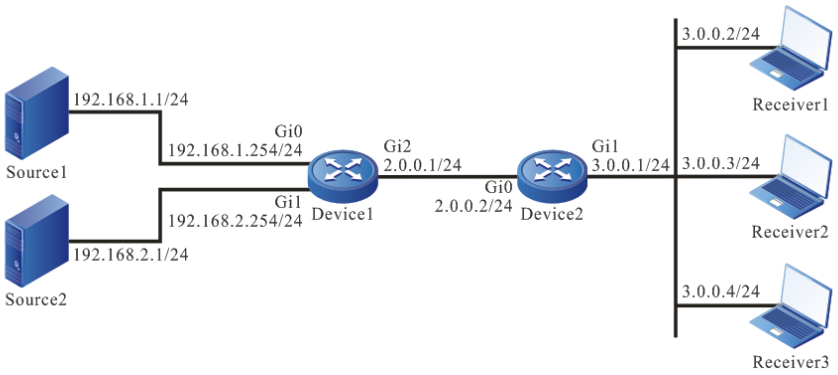


Figure 4-3 Networking of configuring the IGMP SSM mapping

## Configuration Steps

**Step 1:** Configure the IP address of the interface. (omitted)

**Step 2:** Enable the unicast routing OSPF so that all network devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.2.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#View the route table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   2.0.0.0/24 is directly connected, 00:16:05, gigabitethernet0
C   3.0.0.0/24 is directly connected, 00:06:36, gigabitethernet1
O   192.168.1.0/24 [110/2] via 2.0.0.1, 00:15:17, gigabitethernet0
```

```
O   192.168.2.0/24 [110/2] via 2.0.0.1, 00:00:51, gigabitethernet0
```

**Note:**

- The viewing method of Device1 is the same as that of Device2, so the viewing process is omitted.

**Step 3:** Enable the multicast forwarding globally, configure PIM-SSM globally and the multicast group range of the SSM service is 232.0.0.0/8. On the interfaces, enable the multicast protocol PIM-SM. The interface gigabitethernet1 of Device2 runs IGMPv3.

#Configure Device1.

Enable the multicast forwarding globally, configure the PIM-SSM globally and enable the multicast protocol PIM-SM on the interface.

```
Device1(config)#ip multicast-routing
Device1(config)#ip pim ssm default
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip pim sparse-mode
Device1(config-if-gigabitethernet0)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#ip pim sparse-mode
Device1(config-if-gigabitethernet1)#exit
Device1(config)#interface gigabitethernet0/2/2
Device1(config-if-gigabitethernet0/2/2)#ip pim sparse-mode
Device1(config-if-gigabitethernet0/2/2)#exit
```

#Configure Device2.

Enable the multicast forwarding globally, configure the PIM-SSM globally, and enable the multicast protocol PIM-SM on the interface. The interface gigabitethernet1 runs IGMPv3.

```
Device2(config)#ip multicast-routing
Device2(config)#ip pim ssm default
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ip pim sparse-mode
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ip pim sparse-mode
Device2(config-if-gigabitethernet1)#ip igmp version 3
Device2(config-if-gigabitethernet1)#exit
```

#View the IGMP information of the interface gigabitethernet1 on Device2.

```
Device2#show ip igmp interface gigabitethernet1
Interface gigabitethernet1 (Index 50331921)
 IGMP Enabled, Active, Querier (3.0.0.1)
```

```
Configured for version 3
IP router alert option in IGMP V2 msgs: EXCLUDE
Internet address is 3.0.0.1
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
Last member query count is 2
Group Membership interval is 260 seconds
IGMP robustness variable is 2
```

**Step 4:** Enable the IGMP SSM mapping on Device2 and configure the IGMP SSM mapping rule so that Receiver2 and Receiver3 can only receive the multicast service packets sent by Source1.

#Configure Device2.

Enable the IGMP SSM mapping, configure the multicast group range of the IGMP SSM as 232.0.0.0~232.255.255.255, and the multicast source address is 192.168.1.1.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 232.0.0.0 0.255.255.255
Device2(config-std-nacl)#exit
Device2(config)#ip igmp ssm-map enable
Device2(config)#ip igmp ssm-map static 1 192.168.1.1
```

#View the IGMP SSM mapping rule of Device2.

```
Device2#show ip igmp ssm-map

IGMP SSM-MAP Information : enable
acl-name  source-addr
-------------------------
192.168.1.1
```

**Step 5:** Check the result.

# Receiver1 sends the IGMPv3 member report packet of the specified source group to add to the multicast group 232.1.1.1 and the specified multicast source is 192.168.2.1; Receiver2 sends the IGMPv2 member report packet to add to the multicast group 232.1.1.2; Receiver3 sends the IGMPv1 member report packet to add to multicast group 232.1.1.3.

#Source1 and Source2 both send the multicast service packets with multicast groups 232.1.1.1, 232.1.1.2, and 232.1.1.3.

#View the multicast member table.

```
Device2#show ip igmp groups
IGMP Connected Group Membership
Total 3 groups
Group Address    Interface                Uptime    Expires  Last Reporter   V1 Expires
V2 Expires
232.1.1.1        gigabitethernet1         01:28:45  stopped 3.0.0.2         stopped    stopped
232.1.1.2        gigabitethernet1         01:29:01  stopped 3.0.0.3         stopped    stopped
232.1.1.3        gigabitethernet1         01:29:16  stopped 3.0.0.4         stopped    stopped

Device2#show ip igmp groups detail
Interface: gigabitethernet1
Group:          232.1.1.1
Uptime:         01:30:44
Group mode:     Include
Last reporter:  3.0.0.2
TIB-A Count:    1
TIB-B Count:    0
Group source list: (R - Remote, M - SSM Mapping)
 Source Address  Uptime    v3 Exp    M Exp     Fwd  Flags
 192.168.2.1     01:30:44  00:03:39  stopped   Yes  R

Interface: gigabitethernet1
Group:          232.1.1.2
Uptime:         01:31:00
Group mode:     Include
Last reporter:  3.0.0.3
TIB-A Count:    1
TIB-B Count:    0
Group source list: (R - Remote, M - SSM Mapping)
 Source Address  Uptime    v3 Exp    M Exp     Fwd  Flags
 192.168.1.1     01:31:00  stopped   00:03:38  Yes  M

Interface: gigabitethernet1
Group:          232.1.1.3
Uptime:         01:31:15
Group mode:     Include
Last reporter:  3.0.0.4
```

```
TIB-A Count:    1
TIB-B Count:    0
Group source list: (R - Remote, M - SSM Mapping)
  Source Address  Uptime    v3 Exp    M Exp     Fwd  Flags
  192.168.1.1     01:31:15  stopped   00:03:42  Yes  M
```

#View the multicast route table of Device2.

```
Device2#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 3 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(192.168.2.1, 232.1.1.1)
Up time: 01:32:51
KAT time: 00:03:24
RPF nbr: 2.0.0.1
RPF idx: gigabitethernet0
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    gigabitethernet1
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 19868613

(192.168.1.1, 232.1.1.2)
Up time: 01:33:07
KAT time: 00:03:24
```

RPF nbr: 2.0.0.1
RPF idx: gigabitethernet0
SPT bit: TRUE
Flags:
JOIN DESIRED
Upstream State: JOINED
Local interface list:
gigabitethernet1
Joined interface list:
Asserted interface list:
Outgoing interface list:
gigabitethernet1
Packet count 19873645

(192.168.1.1, 232.1.1.3)
Up time: 01:33:22
KAT time: 00:03:24
RPF nbr: 2.0.0.1
RPF idx: gigabitethernet0
SPT bit: TRUE
Flags:
JOIN DESIRED
Upstream State: JOINED
Local interface list:
gigabitethernet1
Joined interface list:
Asserted interface list:
Outgoing interface list:
Gigabitethernet1
Packet count 19873645

# Receiver1 can only receive the multicast service packets sent by Source2; Receiver2 and Receiver3 can only receive the multicast service packets sent by Source1.

**Note:**

- The viewing method of Device1 is the same as that of Device2, so the viewing process is omitted.
- IGMP SSM mapping needs to be used with PIM-SSM; the multicast group range in the IGMP SSM mapping rule should belong to the PIM-SSM multicast group range. IGMP SSM mapping mainly runs IGMPv1 or IGMPv2 and cannot be upgraded to the receiver host of IGMPv3 to provide the supporting for the SSM model.

- The IGMP SSM mapping is invalid for the IGMPv3 member report packet.

### 4.3.4. Configure IGMP Multicast Group Filter

#### Network Requirements

- The whole network runs the PIM-SM protocol.
- Receiver is one receiver of the Device end network.
- Run IGMPv2 between Device and the end network.
- Device interface gigabitethernet1 filters the multicast group; the range of the multicast groups Receiver is permitted to add is 225.1.1.0-225.1.1.255.

#### Network Topology


Figure 4-4 Networking of configuring IGMP multicast group filter

#### Configuration Steps

**Step 1:** Configure the IP address of the interface. (omitted)

**Step 2:** Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

#Configure Device.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related interfaces.

```
Device(config)#configure terminal
Device(config)#ip multicast-routing
Device(config)#interface gigabitethernet0
Device(config-if-gigabitethernet0)#ip pim sparse-mode
Device(config-if-gigabitethernet0)#exit
Device(config)#interface gigabitethernet1
Device(config-if-gigabitethernet1)#ip pim sparse-mode
Device(config-if-gigabitethernet1)#exit
```

#View the IGMP information of Device interface gigabitethernet1.

```
Device#show ip igmp interface gigabitethernet 1
Interface gigabitethernet1 (Index 50331921)
 IGMP Enabled, Active, Querier (3.0.0.1)
 Default version 2
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 3.0.0.1
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
```

```
    IGMP max query response time is 10 seconds
    Last member query response interval is 1 seconds
    Last member query count is 2
    Group Membership interval is 260 seconds
  IGMP robustness variable is 2
```

**Step 3:** Configure the multicast group filter on Device interface gigabitethernet1.

#Configure Device.

Configure the multicast group filter on Device interface gigabitethernet1; the range of the multicast groups Receiver is permitted to add is 225.1.1.0-225.1.1.255.

```
Device(config)#ip access-list standard 1
Device(config-std-nacl)#permit 225.1.1.0 0.0.0.255
Device(config-std-nacl)#exit
Device(config)#interface gigabitethernet1
Device(config-if-gigabitethernet1)#ip igmp access-group 1
Device(config-if-gigabitethernet1)#exit
```

**Step4:** Check the result.

#Receiver sends the IGMPv2 member report packet to add to multicast group 225.1.1.1 and 226.1.1.1.

#Source sends the multicast packets with multicast group 225.1.1.1 and 226.1.1.1.

#View the multicast member table of Device.

```
Device#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address   Interface            Uptime   Expires  Last Reporter  V1 Expires
225.1.1.1       gigabitethernet1     03:14:59 00:03:05 3.0.0.2        stopped
```

#View the multicast route table of Device.

```
Device#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer
```

```
(*, 225.1.1.1)
Up time: 00:00:56
RP: 0.0.0.0
RPF nbr: 0.0.0.0
RPF idx: None
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
  gigabitethernet1
 Joined interface list:
 Asserted interface list:


(192.168.1.1, 225.1.1.1)
Up time: 00:00:15
KAT time: 00:03:15
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: TRUE
Flags:
 JOIN DESIRED
 COULD REGISTER
Upstream State: JOINED
 Local interface list:
 Joined interface list:
  register_vif0
 Asserted interface list:
 Outgoing interface list:
  register_vif0
  gigabitethernet1
 Packet count 1

(192.168.1.1, 225.1.1.1, rpt)
Up time: 00:00:15
```

```
RP: 0.0.0.0
Flags:
  RPT JOIN DESIRED
  RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    gigabitethernet1

(192.168.1.1, 226.1.1.1)
Up time: 00:00:15
KAT time: 00:03:15
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: TRUE
Flags:
  JOIN DESIRED
  COULD REGISTER
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    register_vif0
  Asserted interface list:
  Outgoing interface list:
    register_vif0
  Packet count 1

(192.168.1.1, 226.1.1.1, rpt)
Up time: 00:00:15
RP: 0.0.0.0
Flags:
  RPF SGRPT XG EQUAL
Upstream State: RPT NOT JOINED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
```

#Receiver can only receive the multicast service packets with multicast group 225.1.1.1 sent by Source.

**Note:**

To filter based on multicast source group, use the command ip igmp ssm-access-group to realize. When using the command, it is required that the device runs PIM-SSM and the interface runs IGMPv3.

## 4.3.5. Configure IGMP Proxying

### Network Requirements

- Device1 runs the PIM-SM protocol.
- Receiver is one receiver of the Device2 end network.
- Run IGMPv2 between Device and the end network.
- Device2 is an IGMP proxying device. The IGMP member report packet of the receiver is sent to Device1 through the IGMP proxying interface of Device2, so as to forward the multicast service packet.

### Network Topology

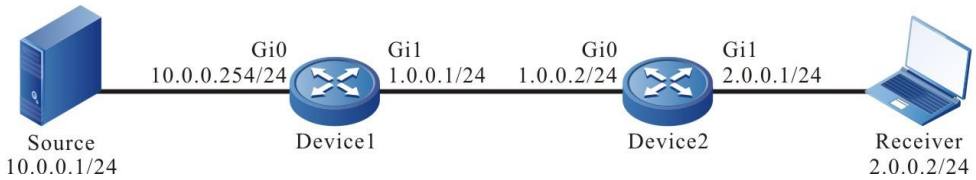


Figure 4-5 Networking of configuring IGMP Proxying

### Configuration Steps

**Step 1:** Configure the IP address of the interface (omitted).

**Step 2:** Enable the unicast routing protocol OSPF, so that all network devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#View the route table of Device2.

```
Device2#show ip route
```

```
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:40:53, gigabitethernet0
C   2.0.0.0/24 is directly connected, 00:04:58, gigabitethernet1
O   10.0.0.0/24 [110/2] via 1.0.0.1, 00:02:59, gigabitethernet0
```

**Note:**

- The viewing method of Device1 is the same as that of Device2, and the viewing process is omitted.

**Step 3:** Enable multicast forwarding globally, and enable multicast protocol PIM-SM on each interface.

#Configure Device1.

Enable multicast forwarding globally, and enable multicast protocol PIM-SM on the corresponding interface.

```
Device1(config)#ip multicast-routing
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip pim sparse-mode
Device1(config-if-gigabitethernet0)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#ip pim sparse-mode
Device1(config-if-gigabitethernet1)#exit
```

#Configure Device2.

Enable multicast forwarding globally, and enable the passive mode of multicast protocol PIM-SM on relevant interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ip pim sparse-mode passive
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ip pim sparse-mode passive
Device2(config-if-gigabitethernet1)#exit
```

#View the IGMP information of the interface gigabitethernet1 of Device2.

```
Device2#show ip igmp interface gigabitethernet 1
Interface gigabitethernet1 (Index 5)
 IGMP Active, Querier (2.0.0.1)
```

```
Default version 2
IP router alert option in IGMP V2 msgs: EXCLUDE
Internet address is 2.0.0.1
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
Last member query count is 2
Group Membership interval is 260 seconds
IGMP robustness variable is 2
```

#View the PIM-SM neighbor information of Device2.

```
Device2#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 0 Neighbor entry
```

**Note:**

- The viewing method of Device1 is the same as that of Device2, and the viewing process is omitted.
- The IGMP function is automatically enabled after the multicast protocol is configured on the interface. After the passive mode of multicast protocol PIM-SM or PIM-DM is enabled on the interface, the interface can normally send and receive IGMP protocol packets without receiving or sending PIM-SM or PIM-DM protocol packets.

**Step 4:** Configure IGMP Proxying.

#Configure Device2.

On gigabitethernet0 of Device2, configure IGMP Proxying.

```
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ip igmp proxying
Device2(config-if-gigabitethernet0)#exit
```

**Step 5:** Check the result.

#Receiver sends IGMPv2 member report packet to join multicast group 225.1.1.1.

#Source sends the multicast service packet with multicast group 225.1.1.1.

#View the multicast member table on device2.

```
Device2#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address   Interface   Uptime   Expires   Last Reporter   V1 Expires   V2 Expires
```

```
225.1.1.1       gigabitethernet1    00:00:02 00:04:18 2.0.0.2          stopped
```

#View the IGMP Proxying multicast member table of Device2.

```
Device2#show ip igmp proxy group
IGMP Proxy Information:
 Upstream Interface: gigabitethernet0
 Upstream Interface Compatible Mode: IGMPv2
 IGMP Proxy Group Membership:
 Total 1 Group Memberships
 ------------------------------
 225.1.1.1
```

#View the IGMP Proxying statics information of Device2.

```
Device2#show ip igmp proxy statistic
IGMP Proxy Report Statistic:
 IGMPv1 Group Member Report Count: 0
 IGMPv2 Group Member Report Count: 3
 IGMPv2 Leave Group Report Count: 0
```

#View the multicast member table on Device1.

```
Device1#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address   Interface          Uptime   Expires  Last Reporter  V1 Expires  V2 Expires
225.1.1.1       gigabitethernet1   00:00:02 00:04:18 1.0.0.2        stopped
```

You can see the multicast group 225.1.1.1 information in the multicast member table of device1, indicating that the IGMP member report packet of Receiver is sent to Device1 through the IGMP proxying interface of Device2.

#Receiver can receive the multicast service packet with multicast group 225.1.1.1 sent by Source.

# 5. PIM-DM

## 5.1. Overview

PIM-DM (Protocol Independent Multicast-Dense Mode) is applicable when the group members are relatively concentrated and the range is small, or the network bandwidth resource is sufficient.

PIM-DM does not depend on the specified unicast route protocol for the RPF check.

PIM-DM adopts the “Push” to transmit the multicast packets. When the multicast source starts to send the multicast packets, suppose that all subnets in the multicast domain have the multicast receivers, so the multicast packets are pushed to all nodes in the network. PIM-DM forwards and prunes the multicast without the receiver. When the node of the pruned multicast forwarding branch node has the receiver of the multicast source, PIM-DM uses the graft mechanism to actively restore the forwarding of the multicast data.

PIM-DM uses the status refresh mechanism to refresh the downstream status regularly so that the pruned branch does not time out.

## 5.2. PIM-DM Function Configuration

Table 5-1 PIM-DM function configuration list

| Configuration Task | |
|---|---|
| Configure PIM-DM basic functions | Configure the PIM-DM protocol |
| Configure the PIM-DM neighbor | Configure the period of sending the HELLO packets |
| | Configure PIM-DM neighbor keepalive time |
| | Configure PIM-DM neighbor filter |
| Configure the status refresh parameters | Configure PIM-DM status refresh interval |

### 5.2.1. Configure PIM-DM Basic Functions

#### Configuration Condition

Before configuring PIM-DM, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, realizing the intra-domain route reachable

### Configure PIM-DM Protocol

Table 5-2 Configure the PIM-DM protocol

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable the IP multicast forwarding | **ip multicast-routing** | Mandatory<br>By default, do not enable the IP multicast forwarding. |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Enable the PIM-DM protocol. | **ip pim dense-mode** | Either<br>By default, PIM-DM is disabled on the interface. |
| | **ip pim dense-mode passive** | |

**Note:**

- After enabling the PIM-DM function, all PIM-DM configurations can take effect.

## 5.2.2. Configure PIM-DM Neighbor

### Configuration Condition

Before configuring the PIM-DM neighbor, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, realizing intra-domain route reachable
- Enable the PIM-DM protocol

### Configure Sending Period of HELLO Packets

The interface enabled with the PIM-DM protocol periodically sends the Hello packets to set up and maintain the PIM-DM neighbor.

Table 5-3 Configure the period of sending HELLO packets

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the period of sending the Hello packets | **ip pim dense-mode hello-interval** *interval-value* | Optional<br>By default, the period of sending the Hello packets is 30s. |

### Configure PIM-DM Neighbor Keepalive Time

When the interface receives the Hello packets of one neighbor, record the holdtime carried in the Hello packet as the keepalive time of the neighbor. If not receiving the Hello packet of the neighbor within the keepalive time, it is regarded that the neighbor becomes invalid.

Table 5-4 Configure PIM-DM neighbor keepalive time

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the keepalive time of the PIM-DM neighbor | **ip pim dense-mode hello-holdtime** *holdtime-value* | Optional<br>By default, the keepalive time of the PIM-DM neighbor is 105s. |

### Configure PIM-DM Neighbor Filter

To save the system resources, you can use the neighbor filter function to set up the neighbor selectively, so as to save the resources of the device.

Table 5-5 Configure the PIM-DM neighbor filter

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the PIM-DM neighbor filter | **ip pim dense-mode neighbor-filter** { *access-list-number* \| *access-list-name* } | Optional<br>By default, do not enable the PIM-DM neighbor filter function. |

## 5.2.3. Configure Status Refresh Parameters

### Configuration Condition

Before configuring the PIM-DM status refresh parameters, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, realizing intra-domain route reachable
- Enable the PIM-DM protocol

### Configure PIM-DM Status Refresh Interval

To prevent the pruned branches from timing out, the devices directly connected to the multicast source periodically send the (S, G) status refresh packet. The packet is forwarded along the initial forwarding path of the PIM-DM hop by hop, so as to refresh the pruning timer status of all devices on the pruned branches.

Table 5-6 Configure the PIM-DM status refresh interval

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the PIM-DM status refresh interval | **ip pim dense-mode state-refresh origination-interval** *interval-value* | Optional<br>By default, the PIM-DM status refresh interval is 60s. |

### 5.2.4. PIM-DM Monitoring and Maintaining

Table 5-7 PIM-DM monitoring and maintaining

| Command | Description |
|---|---|
| **clear ip pim dense-mode mroute** [ *group-address* [ *source-address* ] ] [ **vrf** *vrf-name* ] | Clear the PIM-DM multicast route information. |
| **show ip pim dense-mode interface** [ **detail** ] [ **vrf** *vrf-name* ] | Display the PIM-DM interface information |
| **show ip pim dense-mode neighbor** [ **detail** ] [ **vrf** *vrf-name* ] | Display the PIM-DM neighbor information |
| **show ip pim dense-mode nexthop [** *source-ip-address* ] [ **vrf** *vrf-name* ] | Display the unicast next-hop information from PIM-DM to source |
| **show ip pim dense-mode mroute** [ [ **group** *group-ip-address* ] [ **source** *source-ip-address* ] \| [ **source** *source-ip-address* **group** *source-ip-address* ] ] [ **vrf** *vrf-name* ] | Display the route table information of the PIM-DM protocol |

## 5.3. PIM-DM Typical Configuration Example

### 5.3.1. Configure PIM-DM Basic Functions

#### Network Requirements

- The whole network enables the PIM-DM protocol.
- Receiver is one receiver of the Device2 end network.
- Run IGMPv2 between Device2 and the end network.

#### Network Topology


Figure 5-1 Networking of configuring the PIM-DM basic functions

#### Configuration Steps

**Step 1:** Configure the IP address of the interface. (omitted)

**Step 2:** Enable the unicast route protocol OSPF so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
```

```
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#View the route table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 00:49:46, gigabitethernet0
C   2.0.0.0/24 is directly connected, 01:06:17, gigabitethernet1
O   192.168.1.0/24 [110/2] via 1.0.0.1, 00:01:19, gigabitethernet0
```

**Note:**

- The method of viewing the route table of Device1 is the same as that of Device2.

**Step 3:** Globally enable the multicast forwarding and enable the multicast protocol PIM-DM on the interface.

#Configure Device1.

Globally enable the multicast forwarding and enable the multicast protocol PIM-DM on the interface.

```
Device1(config)#ip multicast-routing
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip pim dense-mode
Device1(config-if-gigabitethernet0)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#ip pim dense-mode
Device1(config-if-gigabitethernet1)#exit
```

#Configure Device2.

Globally enable the multicast forwarding and enable the multicast protocol PIM-DM on the interface.

```
Device2(config)#ip multicast-routing
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ip pim dense-mode
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ip pim dense-mode
Device2(config-if-gigabitethernet1)#exit
```

#View the information of the interface enabled with the PIM-DM protocol on Device2 and the PIM-DM neighbor information.

```
Device2#show ip pim dense-mode interface
Total 2 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry
Address        Interface          VIFIndex  Ver/    Nbr    VIF
                                            Mode    Count  Flag
1.0.0.2        gigabitethernet0   0         v2/D    1      UP
2.0.0.1        gigabitethernet1   1         v2/D    0      UP

Device2#show ip pim dense-mode neighbor
PIM Dense-mode Neighbor Table:
PIM Dense-mode VRF Name: Default
Total 1 Neighbor entries

Neighbor-Address Interface          Uptime/Expires    Ver
1.0.0.1        gigabitethernet0   00:10:42/00:01:36  v2
```

#View the IGMP information of interface gigabitethernet1 of Device2.

```
Device2#show ip igmp interface gigabitethernet1
Interface gigabitethernet1 (Index 50331921)
 IGMP Active, Querier (2.0.0.1)
 Default version 2
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 2.0.0.1
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1 seconds
```

```
Last member query count is 2
Group Membership interval is 260 seconds
IGMP robustness variable is 2
```

**Note:**

- The method of viewing the Device1 information is the same as that of Device2.
- After configuring the multicast protocol on the interface, automatically enable the IGMP function and run IGMPv2 by default. You can configure the running IGMP version on the interface by executing the **ip igmp version** command.

**Step 4:** Check the result.

#Receiver sends the IGMPv2 member report packet to add to multicast group 225.1.1.1.

#Source sends the multicast packets with multicast group 225.1.1.1.

#View the multicast member table of Device2.

```
Device2#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address   Interface        Uptime   Expires  Last Reporter   V1 Expires
225.1.1.1       gigabitethernet1 00:15:07 00:02:09 2.0.0.2         stopped
```

#View the PIM-DM multicast route table of Device2.

```
Device2#show ip pim dense-mode mroute
PIM-DM Multicast Routing Table
Total 1 mroute entry
(192.168.1.1, 225.1.1.1)
  Expire in: 00:03:24
  RPF Neighbor: 1.0.0.1, Nexthop: 1.0.0.1, gigabitethernet0
  Upstream IF: gigabitethernet0
    Upstream State: Forwarding
    Assert State: Loser
  Downstream IF List:
   Gigabitethernet1, in 'olist':
     Downstream State: NoInfo
     Assert State: NoInfo
```

#Receiver can receive the multicast packets with the multicast group 225.1.1.1 sent by Source.

**Note:**

- The method of viewing the Device1 information is the same as that of Device2.

# 6. PIM-SM

## 6.1. Overview

PIM-SM (Protocol Independent Multicast, Sparse Mode) is applicable when the group members are relatively dispersive and their range is relatively broad or the network bandwidth resource is relatively limited.

PIM-SM does not depend on any particular unicast route protocol. The device announces the multicast information to all PIM-SM routers by actively sending the packets to request to set up multicast distributing tree (MDT) and set RP (Rendezvous Point) and BSR (Bootstrap Router). When the receiver adds to one multicast group, the receiving end DR (Designated Router) sends the PIM adding packet to RP, constructing the sharing tree-RPT with RP as root, while the source DR registers the multicast source to RP, constructing the source tree with the multicast source as root. The multicast service packets are transmitted to the receiver along the source tree and sharing tree; the receiving end DR sends the PIM adding packet to the multicast source. At last, switch from RPT to source-based SPT (Shortest-path Tree), so as to reduce the network delay.

PIM SSM is short for Protocol Independent Multicast ---- Source Specific Multicast. PIM-SSM is the subset of the PIM-SM protocol and should run on the basis of PIM-SM. The PIM-SSM protocol set the IPv4 address 232.0.0.0-232.255.255.255 to be reserved for SSM. PIM-SSM should work with IGMPv3, because IGMPv3 can send the IGMP membership report packet of the specified source and group.

## 6.2. PIM-SM Function Configuration

Table 6-1 PIM-SM function configuration list

| **Configuration Task** | |
|---|---|
| Configure the PIM-SM basic functions | Enable the PIM-SM protocol |
| Configure the PIM-SM aggregation router | Configure C-RP |
| | Configure static RP |
| Configure the PIM-SM bootstrap router | Configure C-BSR |
| | Configure the BSR edge |
| Configure PIM-SM multicast source registration | Configure the RP reachability check |
| | Configure the sending rate of the register packets |
| | Configure sending rate of the register stop packets |

| Configuration Task | |
|---|---|
| | Configure the source address of the register packet |
| | Configure register packet filter |
| Configure PIM-SM neighbor parameters | Configure the period of sending the Hello packets |
| | Configure the keepalive time of the neighbor |
| | Configure the neighbor filter |
| | Configure the DR priority |
| Configure PIM-SM SPT switching | Configure the SPT switching condition |
| Configure PIM-SSM | Configure PIM-SSM |
| Configure the PIM adaptive basic function | Configure the PIM adaptive basic function |

### 6.2.1. Configure PIM-SM Basic Functions

#### Configuration Conditions

Before configuring PIM-SM, first complete the following task:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable

### Enable PIM-SM Protocol

Table 6-2 Enable the PIM-SM protocol

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable the IP multicast forwarding | **ip multicast-routing** | Mandatory<br>By default, the IP multicast forwarding is not enabled. |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Enable the PIM-SM protocol | **ip pim sparse-mode** | Either<br>By default, PIM-SM is disabled on the interface. |
| | **ip pim sparse-mode passive** | |

**Note:**

- After enabling the PIM-SM protocol, automatically enable the IGMP protocol.
- After enabling the PIM-SM function, all PIM-SM configurations can take effect.

## 6.2.2. Configure PIM-SM Aggregation Router

### Configuration Condition

Before configuring RP, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Enable the PIM-SM protocol

### Configure C-RP

RP is generated by the C-RO election. After BSR is elected, all C-RPs (Candidate-Rendezvous Point) regularly unicast the C-RP packet to BSR. BSR integrates the C-RP information and transmits the information to all devices in the PIM-SM domain via the bootstrap packet.

Table 6-3 Configure C-RP

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure C-RP | **ip pim rp-candidate** *interface-name* [ [ *priority-value* [ *interval-value* [ **group-list** { *access-list-number* \| *access-list-name* } ] ] ] \| [ **group-list** { *access-list-number* \| *access-list-name* } ] ] [ **vrf** *vrf-name* ] | Mandatory<br>By default, there is no C-RP. |

**Note:**

- RP election rules:
- For the group range of the C-RP service, perform the longest matching of the mask.
- If the longest matching of the mask has multiple C-RPs, compare the C-RP priority. The smaller the value, the high the priority. The one with highest priority wins.
- If there are multiple C-RPs with highest priority, perform the HASH calculation for the C-RP address and group. The one with the largest HASH value wins.
- If there are multiple RPs with the largest HASH, the C-RP with the largest IP address wins.

### Configure Static RP

For the simple PIM-SM network, it is suggested to use the static RP. If using the static RP, do not need to perform the BSR configuration, eliminating the frequent interacting between RP and BSR, so as to save the network bandwidth.

Table 6-4 Configure static RP

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the static RP | **ip pim rp-address** *ip-address* [ *access-list-name* \| *access-list-number* ] [ **override** ] [ **vrf** *vrf-name* ] | Mandatory<br>By default, there is no static RP. |

**Note:**

- All devices in the same PIM-SM domain should be configured with the same static RP.

## 6.2.3. Configure PIM-SM Bootstrap Router

### Configuration Conditions

Before configuring BSR, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Enable the PIM-SM protocol

### Configure C-BSR

In one PIM-SM domain, there should be the unique BSR. Multiple C-BSRs (Candidate-Bootstrap Router) elects to generate the unique BSR via the bootstrap packet.

Table 6-5 Configure C-BSR

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure C-BSR | **ip pim bsr-candidate** *interface_name* [ *hash-mask-length* [ *priority-value* ] ] [ **vrf** *vrf-name* ] | Mandatory<br>By default, there is no C-BSR. |

**Note:**

- BSR election rules:
- Compare the priorities. The larger the value, the higher the priority. The one with highest priority wins.
- If the priority is the same, the one with the largest IP address wins.

### Configure BSR Border

BSR is responsible for collecting the C-RP information and transmits the information to all devices in the PIM-SM domain via the bootstrap packet. The BSR range is the range of the multicast domain. The bootstrap packet cannot pass the interface configured with the BSR border. The devices out of the multicast domain range cannot take part in the forwarding of the multicast service packet in the multicast domain, so as to realize the dividing of the multicast domain.

Table 6-6 Configure the BSR border

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the BSR border | **ip pim bsr-border** | Mandatory<br>By default, there is no multicast border. |

## 6.2.4. Configure PIM-SM Multicast Source Register

### Configuration Condition

Before configuring the multicast source register, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Enable the PIM-SM protocol

### Configure RP Reachability Check

Before source DR sends the register packet to RP, first perform the RP reachability check. If finding that the RP route is not reachable, do not register to RP, so as to reduce the cost of the DR.

Table 6-7 Configure the RP reachability check

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the RP reachability check | **ip pim register-rp-reachability** [ **vrf** *vrf-name* ] | Mandatory<br>By default, before performing the PIM register, do not check the RP reachability. |

**Note:**

- To reduce the cost of the source DR, it is suggested to configure the command on the source DRs of all PIM-SMs.

### Configure Sending Rate of Register Packets

When the source DR receives the multicast packet, encapsulate the multicast packet to the register packet and send to RP for source register until the registration is complete..

When the source DR does not complete the multicast source register and the multicast flow is large, generate lots of register packets, which increase the load of the RP device. Even RP cannot work normally. Source DR does not need to transmit all register packets of one flow to RP, so configuring the rate of sending the register packets at the source DR not only can reach the purpose of source registration, but also can reduce the RP load.

Table 6-8 Configure the rate of sending the register packet

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the rate of sending the register packet | **ip pim register-rate-limit** *rate-limit-value* [ **vrf** *vrf-name* ] | Mandatory<br>By default, do not limit the rate of sending the register packet. |

**Note:**

- To reduce the RP load, it is suggested to configure the rate of sending the source resgiter packets on all source DRs.

**Configure Sending Rate of Register Stop Packets**

After RP receives the register packet of the source DR, send the register stop packet to the source DR to complete the registration. When the RP receives lots of register packets, it is necessary to reply all register packets (send register stop packet). In fact, there are lots of repeated packets in the register stop packets. You can limit the rate of sending the register stop packet on RP to reduce the cost of RP.

Table 6-9 Configure the rate of sending the register stop packet

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the rate of sending the register stop packet | **ip pim register-stop-rate-limit** *rate-limit-value* [ **vrf** *vrf-name* ] | Mandatory<br>By default, do not limit the rate of sending the register stop packet. |

**Note:**

- To improve the robustness of the whole PIM-SM network, it is suggested to limit the rate of the source register stop packet on all RPs.

**Configure Source Address of Register Packet**

When the source DR performs the source register, the source address of the register packet uses the IP address of the register interface automatically registered by the system. The command can specify the source address of the register packet as the IP address of one interface on the device to meet some special demand of the network.

Table 6-10 Configure the source address of the register packet

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the source address of the register packet | **ip pim register-source interface** *interface-name* [ **vrf** *vrf-name* ] | Mandatory<br>By default, use IP address of the register interface automatically registered by the system as the source address of the register packet. |

### Configure Register Packet Filter

To prevent the source register attack, you can use ACL on RP to perform the multicast source filter for the register packet. Only the multicast source permitted by ACL can register successfully on RP.

Table 6-11 Configure the register packet filter

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the register packet filter | **ip pim accept-register list** { *access-list-number* } [ **vrf** *vrf-name* ] | Mandatory<br>By default, do not filter the register packet. |

## 6.2.5. Configure PIM-SM Neighbor Parameters

### Configuration Condition

Before configuring the PIM-SM neighbor parameters, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Enable the PIM-SM protocol

### Configure Sending Period of Hello Packets

The interface enabled with the PIM protocol periodically sends the Hello packets to set up and maintain the PIM neighbor.

Table 6-12 Configure the period of sending the Hello packet

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the period of sending the Hello packet | **ip pim hello-interval** *interval-value* | Optional<br>By default, the period of sending the Hello packet is 30s. |

### Configure Neighbor Keepalive Time

When the interface receives the Hello packets of one neighbor, record the holdtime carried in the Hello packet as the keepalive time of the neighbor. If not receiving the Hello packet of the neighbor within the keepalive time, it is regarded that the neighbor becomes invalid.

Table 6-13 Configure PIM-SM neighbor keepalive time

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure PIM-SM neighbor keepalive time | **ip pim hello-holdtime** *holdtime-value* | Optional<br>By default, the keepalive time of the PIM-SM neighbor is 105s. |

### Configure Neighbor Filter

If there are many PIM neighbors in one subnet, you can use the neighbor filter function to set up the neighbor selectively, so as to save the resources of the device.

Table 6-14 Configure the neighbor filter

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the neighbor filter | **ip pim neighbor-filter** { *access-list-number* \| *access-list-name* } | Mandatory<br>By default, do not enable the neighbor filter function. |

### Configure DR Priority

DR plays one important role in the PIM-SM network, so selecting the appropriate DR is important. You can select the appropriate device as DR by configuring the DR priority.

One PIM-SM subnet only permits one DR. According to the function, DR can be divided to source DR and receiving DR.

The main function of the source DR is to perform the source register to RP.

The main function of the receiving DR is to add to RP and set up the switching of RPT and SPT.

Table 6-15 Configure the DR priority

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the DR priority | **ip pim dr-priority** *priority-value* | Optional<br>By default, the DR priority is 1. |

**Note:**

- DR election rules:
- Compare the priorities. The larger the value, the higher the priority. The one with highest priority wins.
- If the priority is the same, the one with the largest IP address wins.

## 6.2.6. Configure PIM-SM SPT Switching

### Configuration Condition

Before configuring SPT, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Enable the PIM-SM protocol

### Configure SPT Switching Condition

The receiving end DR does not know the address of the multicast source, so it can only add to RP to form RPT. The source DR performs the source register to RP and form the source tree between source DR and RP. At first, the direction of the multicast flow is from multicast source to RP and then from RP to the receiver. When the receiving end DR receives the first multicast packet, it performs adding to multicast source, forms SPT, and performs the pruning for RPT. This is called SPT switching.

The command is to configure the SPT switching condition at the receiving end DR.

Table 6-16 Configure the SPT switching condition

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the SPT switching condition | **ip pim spt-threshold** { **infinity \|** *threshold* [ **group-list** {*access-list-number* \| *access-list-name* } ] [ **vrf** *vrf-name* ] | Mandatory<br>By default, all multicast groups perform the SPT switching. |

**Caution:**

- Do not configure SPT never-switching on RP. Otherwise, it may result in the failure of the multicast forwarding.

## 6.2.7. Configure PIM-SSM

PIM-SSM is one subset of PIM-SM. In PIM-SSM, do not need RP, BSR or RPT, and there is no SPT switching, but the receiving end DR directly adds to multicast source and sets up the shortest path tree (SPT) with source as root.

### Configuration Condition

Before configuring PIM-SSM, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Enable the PIM-SM protocol on all interfaces that need multicast route forwarding

### Configure PIM-SSM

Table 6-17 Configure PIM-SSM

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure PIM-SSM | **ip pim ssm** { **default** \| **range** { *access-list-number* \| *access-list-name* } } [ **vrf** *vrf-name* ] | Mandatory<br>By default, the SSM function is disabled. |

**Caution:**

- When using PIM-SSM, the receiving end should enable IGMPv3.
- When the receiver cannot be upgraded to IGMPv3, you can use the IGMP SSM Mapping function to cooperate with PIM-SSM.
- Ensure that the SSM multicast group address ranges configured on all devices in the domain are consistent. Otherwise, it may result in the abnormality of PIM-SS.

## 6.2.8. Configure PIM Adaptive Basic Function

### Configuration Condition

Before configuring PIM-SDM, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable

### Configure PIM Adaptive Basic Function

Table 6-18 Configure the PIM adaptive basic function

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable the IP multicast forwarding | **ip multicast-routing** [ **vrf** *vrf-name* ] | Mandatory<br>By default, the IP multicast forwarding is disabled. |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the PIM adaptive basic function | **ip pim sparse-dense-mode** | Either<br>By default, the PIM adaptive basic function is disabled. |
| | **ip pim sparse-dense-mode passive** | |

**Note:**

- After enabling the PIM adaptive function on the interface, automatically enable the PIM-SM, PIM-DM, and IGMP protocols.

## 6.2.9. Configure PIM-SM Supporting (*,*,rp)

### Configuration Condition

Before configuring PIM-SM supporting (*,*,rp), first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Enable the PIM-SM protocol

### Enable PIM-SM Supporting (*,*,rp)

Table 6-19 Enable PIM-SM protocol supporting (*,*,rp)

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable the PIM-SM supporting (*,*,rp) | **ip pim mbr [vrf** *vrf-name***]** | Mandatory<br>By default, do not enable the PIM-SM supporting (*,*,rp). |

## 6.2.10. Configure PIM-SM BFD

### Configuration Conditions

Before configuring PIM-SM BFD, first complete the following task:

- Configure the network layer address of the interface, making each neighboring node reachable at the network layer;
- Configure any unicast routing protocol to make intra-domain routing reachable.

### Configure PIM-SM BFD

Table 6-20 Configure PIM-SM BFD

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Enable PIM-SM BFD | **ip pim bfd** | By default, do not enable the PIM-SM BFD function. |

## 6.2.11. PIM-SM Monitoring and Maintaining

Table 6-21 PIM-SM monitoring and maintaining

| Command | Description |
|---|---|
| **clear ip pim bsr rp-set** [ **vrf** *vrf-name* ] | Clear the RP set information of PIM-SM |
| **clear ip pim mroute** [ *group-address* [ *source-address* ] ] [ **vrf** *vrf-name* ] | Clear the multicast route information of PIM-SM |
| **clear ip pim neighbor** [**vrf** *vrf-name* ] | Clear the PIM-SM neighbor information |
| **clear ip pim stat** [ [ **interface** *interface-name* \| [ **all_interface** ] ] \| [ **vrf** *vrf-name* ] ] | Clear the statics information of the PIM-SM protocol packets |
| **show ip pim bsr-router** [ **vrf** *vrf-name* ] | Display the PIM-SM bootstrap route information |
| **show ip pim interface** [ **detail** ] [ **vrf** *vrf-name* ] | Display the PIM-SM interface information |
| **show ip pim local-members** *interface-name* [ **vrf** *vrf-name* ] | Display the PIM-SM local group member information |
| **show ip pim mroute** [ **active** \| **proxy** \| **ssm** [ **active** ] \| **group** *group-address* [ **source** | Display the PIM-SM multicast route table information |

| Command | Description |
|---|---|
| *source-address* ] \| **source** *source-address* ] [ **vrf** *vrf-name* ] | |
| **show ip pim neighbor** [ **detail** ] [ **vrf** *vrf-name* ] | Display the PIM-SM neighbor information |
| **show ip pim nexthop** [ *ip-address* ] [ **vrf** *vrf-name* ] | Display the PIM-SM next-hop router information |
| **show ip pim rp mapping** [ **vrf** *vrf-name* ] | Display the PIM-SM RP information |
| **show ip pim rp-hash** *group-address* [ **vrf** *vrf-name* ] | Display the RP information of the multicast group mapping |
| **show ip pim statistics** [ **vrf** *vrf-name* ] | Display the statistics information of the PIM-SM protocol packets |

## 6.3. PIM-SM Typical Configuration Example

### 6.3.1. Configure PIM-SM Basic Functions

#### Network Requirements

- The whole network runs the PIM-SM protocol.
- Receiver1 and Receiver2 are the two receivers of Device3 end network.
- Device1 and Device2 are C-BSR and C-RP.
- Run IGMPv2 between Device3 and the end network.

#### Network Topology

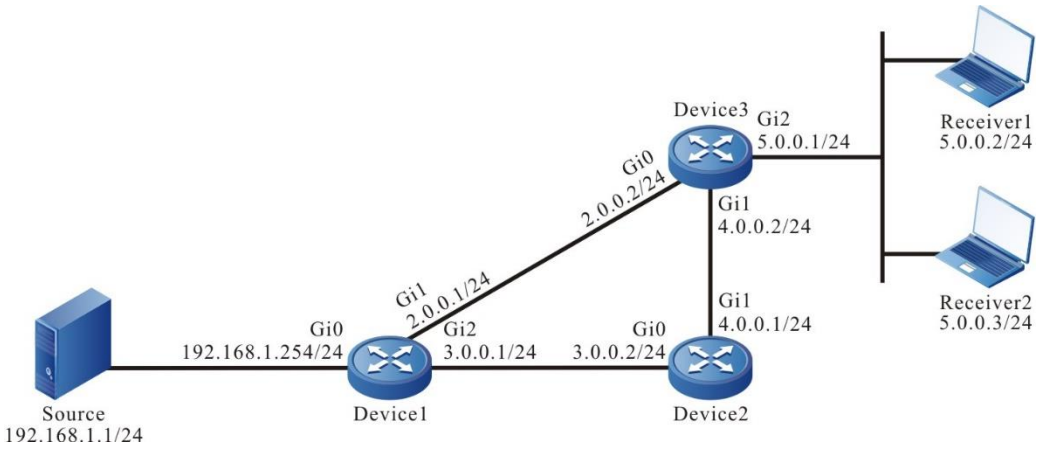


Figure 6-1 Networking of configuring PIM-SM basic functions

## Configuration Steps

**Step 1:** Configure the IP address of the interface. (omitted)

**Step 2:** Enable the unicast route protocol OSPF so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#View the route table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
```

```
C   2.0.0.0/24 is directly connected, 23:48:47, gigabitethernet0
O   3.0.0.0/24 [110/2] via 2.0.0.1, 23:31:14, gigabitethernet0
                [110/2] via 4.0.0.1, 23:31:04, gigabitethernet1
C   4.0.0.0/24 is directly connected, 23:36:57, gigabitethernet1
C   5.0.0.0/24 is directly connected, 23:09:18, gigabitethernet0/2/2
O   192.168.1.0/24 [110/2] via 2.0.0.1, 00:30:55, gigabitethernet0
```

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

**Step 3:** Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

#Configure Device1.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip pim sparse-mode
Device1(config-if-gigabitethernet0)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#ip pim sparse-mode
Device1(config-if-gigabitethernet1)#exit
Device1(config)#interface gigabitethernet0/2/2
Device1(config-if-gigabitethernet0/2/2)#ip pim sparse-mode
Device1(config-if-gigabitethernet0/2/2)#exit
```

#Configure Device2.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ip pim sparse-mode
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ip pim sparse-mode
Device2(config-if-gigabitethernet1)#exit
```

#Configure Device3.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related interfaces.

```
Device3(config)#ip multicast-routing
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#ip pim sparse-mode
Device3(config-if-gigabitethernet0)#exit
Device3(config)#interface gigabitethernet1
Device3(config-if-gigabitethernet1)#ip pim sparse-mode
Device3(config-if-gigabitethernet1)#exit
Device3(config)#interface gigabitethernet0/2/2
Device3(config-if-gigabitethernet0/2/2)#ip pim sparse-mode
Device3(config-if-gigabitethernet0/2/2)#exit
```

#View the information of the interface enabled with the PIM-SM protocol on Device3 and the PIM-SM neighbor information.

```
Device3#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 4 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address         Interface            VIF     Ver/   VIF   Nbr    DR    DR          BSR
CISCO    Neighbor
                                     Index   Mode   Flag  Count  Pri             Border Neighbor
Filter
2.0.0.2         register_vif0        1       v2/S   UP
2.0.0.2         gigabitethernet0     0       v2/S   UP    1      2     2.0.0.2     FALSE
FALSE
4.0.0.2         gigabitethernet1     2       v2/S   UP    0      1     4.0.0.2     FALSE
FALSE
5.0.0.1         gigabitethernet0/2/2 3       v2/S   UP    0      1     5.0.0.1     FALSE
FALSE

Device3#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 2 Neighbor entries
Neighbor        Interface            Uptime/Expires    Ver   DR
Address
2.0.0.1         gigabitethernet0     01:12:00/00:01:39 v2    1 /
4.0.0.1         gigabitethernet1     01:13:19/00:01:35 v2    1 /
```

**Note:**

- The viewing methods of Device1 and Device2 are the same as that of Device3, so the viewing process is omitted.

#View the IGMP information of interface gigabitethernet0/2/2 of Device3.

```
Device3#show ip igmp interface gigabitethernet0/2/2
Interface gigabitethernet0/2/2 (Index 50332250)
 IGMP Active, Querier (5.0.0.1)
 Default version 2
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 5.0.0.1
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1 seconds
 Last member query count is 2
 Group Membership interval is 260 seconds
 IGMP robustness variable is 2
```

**Caution:**

- After configuring the multicast protocol on the interface, automatically enable the IGMP function and run IGMPv2 by default. You can configure the running IGMP version on the interface by **executing the ip igmp version** command.

**Step 4:** Configure the interface gigabitethernet1 of Device1 as C-BSR and C-RP, and configure the interface gigabitethernet0 of Device2 as C-BSR and C-RP.

#Configure Device1.

Configure interface gigabitethernet1 of Device1 as C-BSR and C-RP; the priority of C-BSR is 200; the multicast group range of the C-RP service is 230.0.0.0/8.

```
Device1(config)#ip pim bsr-candidate gigabitethernet1 10 200
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 230.0.0.0 0.255.255.255
Device1(config-std-nacl)#exit
Device1(config)#ip pim rp-candidate gigabitethernet1 group-list 1
```

#Configure Device2.

Configure interface gigabitethernet0 of Device2 as C-BSR and C-RP; the priority of C-BSR is 0; the multicast group range of the C-RP service of Device2 is 230.0.0.0/4.

```
Device2(config)#ip pim bsr-candidate gigabitethernet0
Device2(config)#ip pim rp-candidate gigabitethernet0
```

#View the BSR and RP information of Device3.

```
Device3#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
  BSR address: 2.0.0.1
  BSR Priority: 200
  Hash mask length: 10
  Up time: 01:03:30
  Expiry time: 00:01:46
  Role: Non-candidate BSR
  State: Accept Preferred

Device3#show ip pim rp mapping
PIM Group-to-RP Mappings Table:
PIM VRF Name: Default
Total 2 RP set entries
Total 2 RP entries

  Group(s): 224.0.0.0/4
  RP count: 1
    RP: 3.0.0.2
      Info source: 2.0.0.1, via bootstrap, priority 192
      Up time: 01:03:29
      Expiry time: 00:02:02

  Group(s): 230.0.0.0/8
  RP count: 1
    RP: 2.0.0.1
      Info source: 2.0.0.1, via bootstrap, priority 192
      Up time: 01:15:50
      Expiry time: 00:02:02
```

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.
- When configuring multiple C-BSRs in one multicast domain, first elect BSR according to the priority and the C-BSR with the largest priority is elected as BSR. When the priorities of C-BSRs are the same, the C-BSR with the largest ip address is elected as BSR.

- When configuring multiple C-RPs in one multicast domain and the service multicast group ranges are the same, calculate the RP of the multicast group G according to the hash algorithm.

In the multicast domain, you can configure RP via the command ip **pim rp-address**, but it is required that the static RP addresses configured on all devices in the multicast domain keep consistent.

**Step 5:** Check the result.

# Receiver1 and Receiver2 send the IGMPv2 member report packet to add to multicast group 225.1.1.1, 230.1.1.1 respectively.

#Source sends the multicast packets with multicast group 225.1.1.1, 230.1.1.1.

#View the multicast member table of Device3.

```
Device3#show ip igmp groups
IGMP Connected Group Membership
Total 2 groups
Group Address   Interface          Uptime   Expires  Last Reporter   V1 Expires
225.1.1.1       gigabitethernet0/2/2   00:56:48 00:02:39 5.0.0.2         stopped
230.1.1.1       gigabitethernet0/2/2   00:56:48 00:02:46 5.0.0.3         stopped
```

#View the RP of multicast group 225.1.1.1,230.1.1.1 on Device3.

```
Device3#show ip pim rp-hash 225.1.1.1
 PIM VRF Name: Default
 RP: 3.0.0.2
   Info source: 2.0.0.1, via bootstrap

Device3#show ip pim rp-hash 230.1.1.1
 PIM VRF Name: Default
 RP: 2.0.0.1
   Info source: 2.0.0.1, via bootstrap
```

#View the multicast route table of Device3.

```
Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 2 (*,G) entries
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer
```

(*, 225.1.1.1)
Up time: 00:36:21
RP: 3.0.0.2
RPF nbr: 4.0.0.1
RPF idx: gigabitethernet1
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
  gigabitethernet0/2/2
 Joined interface list:
 Asserted interface list:

(192.168.1.1, 225.1.1.1)
Up time: 00:36:02
KAT time: 00:03:11
RPF nbr: 2.0.0.1
RPF idx: gigabitethernet0
SPT bit: TRUE
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
 Joined interface list:
 Asserted interface list:
 Outgoing interface list:
  gigabitethernet0/2/2
 Packet count 2517423

(192.168.1.1, 225.1.1.1, rpt)
Up time: 00:36:02
RP: 3.0.0.2
Flags:
 RPT JOIN DESIRED

PRUNE DESIRED
RPF SGRPT XG EQUAL
Upstream State: PRUNED
Local interface list:
Pruned interface list:
Outgoing interface list:
gigabitethernet0/2/2

(*, 230.1.1.1)
Up time: 00:36:21
RP: 2.0.0.1
RPF nbr: 2.0.0.1
RPF idx: gigabitethernet0
Flags:
JOIN DESIRED
Upstream State: JOINED
Local interface list:
gigabitethernet0/2/2
Joined interface list:
Asserted interface list:

(192.168.1.1, 230.1.1.1)
Up time: 00:36:02
KAT time: 00:03:11
RPF nbr: 2.0.0.1
RPF idx: gigabitethernet0
SPT bit: TRUE
Flags:
JOIN DESIRED
Upstream State: JOINED
Local interface list:
Joined interface list:
Asserted interface list:
Outgoing interface list:
gigabitethernet0/2/2
Packet count 2517712

(192.168.1.1, 230.1.1.1, rpt)

Up time: 00:36:02

RP: 2.0.0.1

Flags:

RPT JOIN DESIRED

RPF SGRPT XG EQUAL

Upstream State: NOT PRUNED

Local interface list:

Pruned interface list:

Outgoing interface list:

#Receiver1 can only receive the multicast service packet with multicast group 225.1.1.1 sent by Source. Receiver2 can only receive the multicast service packet with multicast group 230.1.1.1 sent by Source.

**Note:**

- The viewing method of Device1 and Device2 is the same as that of Device3, so the viewing process is omitted.
- By default, the device enables the SPT switching.

## 6.3.2. Configure PIM-SSM

### Network Requirements

- The whole network runs the PIM-SSM protocol.
- Receiver is one receiver of Device3 end network.
- Run IGMPv3 between Device3 and the end network.

### Network Topology

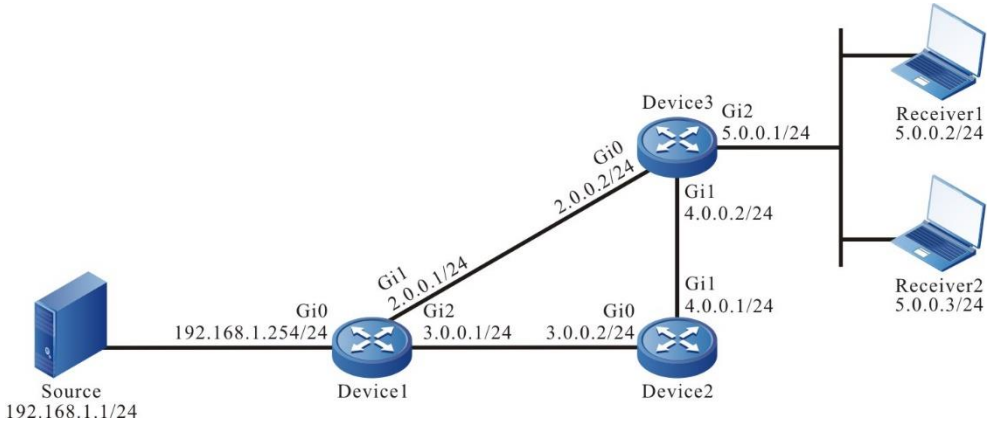


Figure 6-2 Networking of configuring PIM-SSM

### Configuration Steps

**Step 1:** Configure the IP address of the interface. (omitted)

**Step 2:** Enable the unicast route protocol OSPF so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#View the route table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   2.0.0.0/24 is directly connected, 23:48:47, gigabitethernet0
O   3.0.0.0/24 [110/2] via 2.0.0.1, 23:31:14, gigabitethernet1
              [110/2] via 4.0.0.1, 23:31:04, gigabitethernet1
C   4.0.0.0/24 is directly connected, 23:36:57, gigabitethernet1
C   5.0.0.0/24 is directly connected, 23:09:18, gigabitethernet0/2/2
O   192.168.1.0/24 [110/2] via 2.0.0.1, 00:30:55, gigabitethernet0
```

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

**Step 3:** Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

#Configure Device1.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip pim sparse-mode
Device1(config-if-gigabitethernet0)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#ip pim sparse-mode
Device1(config-if-gigabitethernet1)#exit
Device1(config)#interface gigabitethernet0/2/2
Device1(config-if-gigabitethernet0/2/2)#ip pim sparse-mode
Device1(config-if-gigabitethernet0/2/2)#exit
```

#Configure Device2.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ip pim sparse-mode
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ip pim sparse-mode
Device2(config-if-gigabitethernet1)#exit
```

#Configure Device3.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related interfaces.

```
Device3(config)#ip multicast-routing
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#ip pim sparse-mode
Device3(config-if-gigabitethernet0)#exit
Device3(config)#interface gigabitethernet1
```

```
Device3(config-if-gigabitethernet1)#ip pim sparse-mode
Device3(config-if-gigabitethernet1)#exit
Device3(config)#interface gigabitethernet0/2/2
Device3(config-if-gigabitethernet0/2/2)#ip pim sparse-mode
Device3(config-if-gigabitethernet0/2/2)#exit
```

#View the information of the interface enabled with the PIM-SM protocol on Device3 and the PIM-SM neighbor information.

```
Device3#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 4 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address         Interface            VIF     Ver/  VIF   Nbr    DR    DR          BSR
CISCO    Neighbor
                                     Index   Mode  Flag  Count  Pri             Border Neighbor
Filter
2.0.0.2         register_vif0        1       v2/S  UP
2.0.0.2         gigabitethernet0     3       v2/S  UP    1      1     2.0.0.2     FALSE
FALSE
4.0.0.2         gigabitethernet1     0       v2/S  UP    0      1     4.0.0.2     FALSE
FALSE
5.0.0.1         gigabitethernet0/2/2 2       v2/S  UP    1      1     5.0.0.1     FALSE
FALSE

Device3#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 2 Neighbor entries
Neighbor        Interface            Uptime/Expires    Ver   DR
Address
2.0.0.1         gigabitethernet0     01:12:00/00:01:39 v2    1 /
4.0.0.1         gigabitethernet1     01:13:19/00:01:35 v2    1 /
```

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

**Step 4:** Configure PIM-SSM on all devices; the multicast group range of the SSM service is 232.0.0.0/8. gigabitethernet0/2/2 of Device3 runs IGMPv3.

#Configure Device1.

```
Device1(config)#ip pim ssm default
```

#Configure Device2.

```
Device2(config)#ip pim ssm default
```

#Configure Device3.

```
Device3(config)#ip pim ssm default
Device3(config)#interface gigabitethernet0/2/2
Device3(config-if-gigabitethernet0/2/2)#ip igmp version 3
Device3(config-if-gigabitethernet0/2/2)#exit
```

#View the IGMP information of interface gigabitethernet0/2/2 of Device3.

```
Device3#show ip igmp interface gigabitethernet0/2/2
Interface gigabitethernet0/2/2 (Index 50332250)
 IGMP Enabled, Active, Querier (5.0.0.1)
 Configured for version 3
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 5.0.0.1
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1 seconds
 Last member query count is 2
 Group Membership interval is 260 seconds
 IGMP robustness variable is 2
```

**Step 5:** Check the result.

#Receiver sends the IMGPv3 member relation report of the specified source group to add to multicast group 232.1.1.1; the specified multicast source is 192.168.1.1

#Source sends the multicast packets with multicast group 232.1.1.1.

#View the multicast member table of Device3.

```
Device3#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address   Interface          Uptime   Expires  Last Reporter  V1 Expires  V2 Expires
232.1.1.1       gigabitethernet0/2/2  00:11:14  stopped  5.0.0.2        stopped     stopped
```

```
Device3#show ip igmp groups detail
Interface:     gigabitethernet0/2/2
Group:         232.1.1.1
Uptime:        00:11:20
Group mode:    Include
Last reporter:  5.0.0.2
TIB-A Count:    1
TIB-B Count:    0
Group source list: (R - Remote, M - SSM Mapping)
  Source Address  Uptime    v3 Exp    M Exp     Fwd  Flags
  192.168.1.1     00:11:20  00:03:28  stopped   Yes  R
```

#View the multicast route table of Device3.

```
Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entry
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(192.168.1.1, 232.1.1.1)
Up time: 12:59:27
KAT time: 00:03:20
RPF nbr: 2.0.0.1
RPF idx: gigabitethernet0
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
   gigabitethernet0/2/2
  Joined interface list:
  Asserted interface list:
```

```
Outgoing interface list:
  gigabitethernet0/2/2
Packet count 109783214
```

#Receiver can only receive the multicast service packet with multicast group 232.1.1.1 sent by Source.

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.
- The default multicast group range of PIM-SSM is 232.0.0.0/8. You can modify the multicast group range of the 232.0.0.0/8 service via the command ip pim ssm range.
- For the multicast group G meeting the SSM condition, the multicast route table does not generate the (*,G) entry, but just generate the (S,G) entry.

## 6.3.3. Configure PIM-SM Multicast Forwarding Control

### Network Requirements

- The whole network runs the PIM-SM protocol.
- Receiver is one receiver of Device3 end network.
- Device2 is C-BSR and C-RP.
- On Device2 and Device3, control for the multicast source, making Receiver only receive the multicast service packet sent by Source1.
- Run IGMPv2 between Device3 and the end network.

### Network Topology

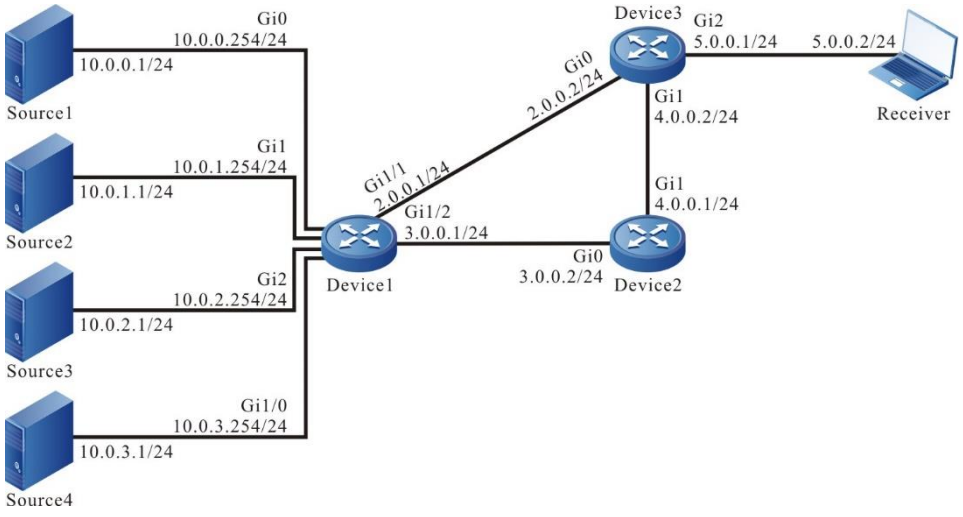


Figure 6-3 Networking of configuring PIM-SM multicast forwarding control

### Configuration Steps

**Step 1:** Configure the IP address of the interface. (omitted)

**Step 2:** Enable the unicast route protocol OSPF so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.0.0 0.0.255.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#View the route table of Device3.

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   2.0.0.0/24 is directly connected, 23:51:07, gigabitethernet0
O   3.0.0.0/24 [110/2] via 2.0.0.1, 23:33:34, gigabitethernet0
              [110/2] via 4.0.0.1, 23:33:24, gigabitethernet1
C   4.0.0.0/24 is directly connected, 23:39:17, gigabitethernet1
C   5.0.0.0/24 is directly connected, 23:11:38, gigabitethernet0/2/2
O   10.0.0.0/24 [110/2] via 2.0.0.1, 00:06:32, gigabitethernet0
O   10.0.1.0/24 [110/2] via 2.0.0.1, 00:06:32, gigabitethernet0
O   10.0.2.0/24 [110/2] via 2.0.0.1, 00:06:32, gigabitethernet0
```

```
O   10.0.3.0/24 [110/2] via 2.0.0.1, 00:06:32, gigabitethernet0
```

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

**Step 3:** Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

#Configure Device1.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip pim sparse-mode
Device1(config-if-gigabitethernet0)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#ip pim sparse-mode
Device1(config-if-gigabitethernet1)#exit
Device1(config)#interface gigabitethernet0/2/2
Device1(config-if-gigabitethernet0/2/2)#ip pim sparse-mode
Device1(config-if-gigabitethernet0/2/2)#exit
Device1(config)#interface gigabitethernet1/0
Device1(config-if-gigabitethernet1/0)#ip pim sparse-mode
Device1(config-if-gigabitethernet1/0)#exit
Device1(config)#interface gigabitethernet1/1
Device1(config-if-gigabitethernet1/1)#ip pim sparse-mode
Device1(config-if-gigabitethernet1/1)#exit
Device1(config)#interface gigabitethernet1/2
Device1(config-if-gigabitethernet1/2)#ip pim sparse-mode
Device1(config-if-gigabitethernet1/2)#exit
```

#Configure Device2.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related interfaces.

```
Device2(config)#ip multicast-routing
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ip pim sparse-mode
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ip pim sparse-mode
```

```
Device2(config-if-gigabitethernet1)#exit
```

#Configure Device3.

Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the related interfaces.

```
Device3(config)#ip multicast-routing
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#ip pim sparse-mode
Device3(config-if-gigabitethernet0)#exit
Device3(config)#interface gigabitethernet1
Device3(config-if-gigabitethernet1)#ip pim sparse-mode
Device3(config-if-gigabitethernet1)#exit
Device3(config)#interface gigabitethernet0/2/2
Device3(config-if-gigabitethernet0/2/2)#ip pim sparse-mode
Device3(config-if-gigabitethernet0/2/2)#exit
```

#View the information of the interface enabled with the PIM-SM protocol on Device3 and the PIM-SM neighbor information.

```
Device3#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 4 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address         Interface           VIF    Ver/  VIF   Nbr   DR       DR          BSR
CISCO   Neighbor
                                    Index  Mode  Flag  Count Priority             Border
Neighbor    Filter
4.0.0.2         register_vif0       1      v2/S  UP
2.0.0.2         gigabitethernet0    2      v2/S  UP    1     2        2.0.0.2     FALSE
FALSE
4.0.0.2         gigabitethernet1    0      v2/S  UP    1     1        4.0.0.2     FALSE
FALSE
5.0.0.1         gigabitethernet0/2/2 3     v2/S  UP    0     1        5.0.0.1     FALSE
FALSE

Device3#show ip pim neighbor
PIM Neighbor Table:
```

```
PIM VRF Name: Default
Total 2 Neighbor entries

Neighbor        Interface          Uptime/Expires    Ver   DR
Address                                              Priority/Mode
2.0.0.1         gigabitethernet0   00:50:29/00:01:19 v2    1 /
4.0.0.1         gigabitethernet1   00:57:58/00:01:33 v2    1 /
```

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

**Step 4:** Configure gigabitethernet0 of Device2 as the C-BSR and C-RP of the whole network and the multicast group range of the C-RP service is 224.0.0.0/4.

#Configure Device2.

```
Device2(config)#ip pim bsr-candidate gigabitethernet0
Device2(config)#ip pim rp-candidate gigabitethernet0
```

#View the BSR and RP information of Device3.

```
Device3#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
  BSR address: 3.0.0.2
  BSR Priority: 0
  Hash mask length: 10
  Up time: 00:10:37
  Expiry time: 00:01:33
  Role: Non-candidate BSR
  State: Accept Preferred

Device3#show ip pim rp mapping
PIM Group-to-RP Mappings Table:
PIM VRF Name: Default
Total 1 RP set entry
Total 1 RP entry

  Group(s): 224.0.0.0/4
  RP count: 1
    RP: 3.0.0.2
      Info source: 3.0.0.2, via bootstrap, priority 192
```

```
Up time: 03:59:59
Expiry time: 00:01:49
```

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

**Step 5:** On Device2 and Device3, control for the multicast source, making Receiver only receive the multicast service packet sent by Source1

#On Device2, configure the accepted register message access list, filtering the register message of Source4.

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#deny 10.0.3.0 0.0.0.255
Device2(config-std-nacl)#permit any
Device2(config-std-nacl)#exit
Device2(config)#ip pim accept-register list 1
```

#On interface gigabitethernet0 and gigabitethernet1 of Device3, configure the ingress acl, filtering the multicast service packets of Source3.

```
Device3(config)#ip access-list extended 1001
Device3(config-ext-nacl)#deny ip 10.0.2.0 0.0.0.255 224.0.0.0 31.255.255.255
Device3(config-ext-nacl)#permit igmp any any
Device3(config-ext-nacl)#permit pim any any
Device3(config-ext-nacl)#permit ospf any any
Device3(config-ext-nacl)#permit ip any any
Device3(config-ext-nacl)#exit
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#ip access-group 1001 in
Device3(config-if-gigabitethernet0)#exit
Device3(config)#interface gigabitethernet1
Device3(config-if-gigabitethernet1)#ip access-group 1001 in
Device3(config-if-gigabitethernet1)#exit
```

#On interface gigabitethernet0/2/2 of Device3, configure the ingress acl, filtering the multicast service packets of Source2.

```
Device3(config)#ip access-list extended 1002
Device3(config-ext-nacl)#deny ip 10.0.1.0 0.0.0.255 224.0.0.0 31.255.255.255
Device3(config-ext-nacl)#permit igmp any any
Device3(config-ext-nacl)#permit pim any any
Device3(config-ext-nacl)#permit ip any any
Device3(config-ext-nacl)#exit
Device3(config)#interface gigabitethernet0/2/2
```

```
Device3(config-if-gigabitethernet0/2/2)#ip access-group 1002 out
Device3(config-if-gigabitethernet0/2/2)#exit
```

**Step 6:** Check the result.

#Receiver sends the IMGPv2 member relation report to add to multicast group 225.1.1.1.

# Source1, Source2, Source3, and Source4 all send the multicast packets of multicast group 225.1.1.1.

#View the multicast member table of Device3.

```
Device3#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address   Interface          Uptime   Expires  Last Reporter   V1 Expires
225.1.1.1       gigabitethernet0/2/2   00:00:38 00:03:45 5.0.0.2         stopped
```

#View the multicast route table of Device3.

```
Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer


(*, 225.1.1.1)
Up time: 00:07:55
RP: 3.0.0.2
RPF nbr: 4.0.0.1
RPF idx: gigabitethernet1
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    gigabitethernet0/2/2
  Joined interface list:
  Asserted interface list:
```

(10.0.0.1, 225.1.1.1)
Up time: 00:07:49
KAT time: 00:03:17
RPF nbr: 2.0.0.1
RPF idx: gigabitethernet0
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet0/2/2
  Packet count 268411

(10.0.0.1, 225.1.1.1, rpt)
Up time: 00:07:49
RP: 3.0.0.2
Flags:
  RPT JOIN DESIRED
  PRUNE DESIRED
  RPF SGRPT XG EQUAL
Upstream State: PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    gigabitethernet0/2/2

(10.0.1.1, 225.1.1.1)
Up time: 00:07:49
KAT time: 00:03:17
RPF nbr: 2.0.0.1
RPF idx: gigabitethernet0
SPT bit: TRUE

```
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
   gigabitethernet0/2/2
  Packet count 268237

(10.0.1.1, 225.1.1.1, rpt)
Up time: 00:07:49
RP: 3.0.0.2
Flags:
  RPT JOIN DESIRED
  PRUNE DESIRED
  RPF SGRPT XG EQUAL
Upstream State: PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
gigabitethernet0/2/2
```

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

#View the matching of ACL on Device2.

```
Device2#show ip access-list 1
ip access-list standard 1
 10 deny 10.0.3.0 0.0.0.255     32 matches
 20 permit any     2767 matches
```

#View the matching of ACL on Device3.

```
Device3#show ip access-list  1001
ip access-list extended 1001
 10 deny ip 10.0.2.0 0.0.0.255 224.0.0.0 31.255.255.255     671545 matches
 20 permit igmp any any     19 matches
 30 permit pim any any     119 matches
 40 permit ospf any any     252 matches
```

```
50 permit ip any any     1343339 matches
```

```
Device3#show ip access-list  1002
ip access-list extended 1002
 10 deny ip 10.0.1.0 0.0.0.255 224.0.0.0 31.255.255.255     672358 matches
 20 permit igmp any any     10 matches
 30 permit pim any any     40 matches
 40 permit ip any any     672532 matches
```

#Receive end can only receive the multicast service packets sent by Source1.

**Caution:**

- When performing the multicast source control, you'd better first configure the multicast source control and then on-demand multicast source, because by default, after receiving the multicast service packet, the receiving end DR performs the SPT switching. If first on-demanding multicast source and then performing the multicast forwarding control, the multicast forwarding control does not take function. To prevent the multicast forwarding control from not taking function, you can configure not permitting SPT switching on the receiving end DR.

## 6.3.4. Configure PIM Adaptive Function

### Network Requirements

- On all interfaces of Device1 and Device2, enable the PIM adaptive function.
- Device1 is C-BSR and C-RP; the multicast group range of the C-RP service is 225.0.0.0/8.
- Run IGMPv2 between Device2 and the end network.
- Receiver is one receiver of Device2 end network.

### Network Topology

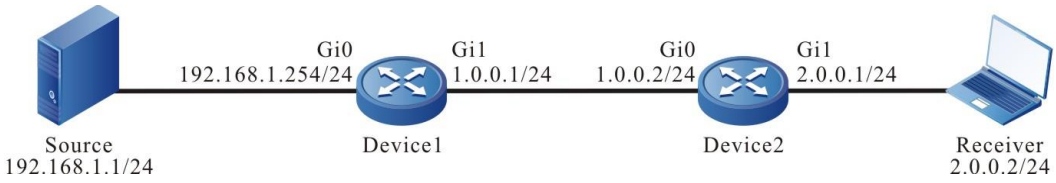


Figure 6-4 Networking of configuring PIM adaptive function

### Configuration Steps

**Step 1:** Configure the IP address of the interface. (omitted)

**Step 2:** Enable the unicast route protocol OSPF so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
```

```
Device1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#View the route table of Device2.

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   1.0.0.0/24 is directly connected, 15:00:16, gigabitethernet0
C   2.0.0.0/24 is directly connected, 01:09:58, gigabitethernet1
    192.168.1.0/24 [110/2] via 1.0.0.1, 00:18:44, gigabitethernet0
```

**Note:**

- The viewing method of Device1 is the same as that of Device2, so the viewing process is omitted.

**Step 3:** Globally enable the multicast forwarding; enable the PIM adaptive function on the interface.

#Configure Device1.

Globally enable the multicast forwarding; enable the PIM adaptive function on the related interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip pim sparse-dense-mode
Device1(config-if-gigabitethernet0)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#ip pim sparse-dense-mode
Device1(config-if-gigabitethernet1)#exit
```

#Configure Device2.

Globally enable the multicast forwarding; enable the PIM adaptive function on the related interfaces.

```
Device2(config)#ip multicast-routing
```

```
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ip pim sparse-dense-mode
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ip pim sparse-dense-mode
Device2(config-if-gigabitethernet1)#exit
```

**Note:**

- After enabling the PIM adaptive function on the interface, automatically enable the PIM-SM and PIM-DM protocols.

#View the information of the interface enabled with the PIM-SM protocol on Device2 and the PIM-SM neighbor information.

```
Device2#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 3 Interface entries
Total 0 External Interface entry
Total 3 Sparse-Dense Mode Interface entries

Address      Interface      VIF    Ver/   VIF  Nbr   DR      DR          BSR   CISCO
Neighbor
                            Index  Mode   Flag Count Priority            Border Neighbor
Filter
2.0.0.1      register_vif0  1      v2/S   UP
1.0.0.2      gigabitethernet0  2   v2/S   UP   1     1       1.0.0.2     FALSE FALSE
2.0.0.1      gigabitethernet1  0   v2/S   UP   0     1       2.0.0.1     FALSE FALSE

Device2#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 1 Neighbor entry

Neighbor      Interface      Uptime/Expires   Ver   DR
Address                                       Priority/Mode
1.0.0.1       gigabitethernet0  00:12:31/00:01:44 v2   N /
```

#We can see that the PIM-SM neighbor is set up between Device2 and Device1 successfully.

#View the information of the interface enabled with the PIM-DM protocol on Device2 and the PIM-DM neighbor information.

```
Device2#show ip pim dense-mode interface
```

```
Total 2 Interface entries
Total 0 External Interface entry
Total 2 Sparse-Dense Mode Interface entries
Address      Interface        VIFIndex   Ver/    Nbr    VIF
                                        Mode    Count  Flag
1.0.0.2      gigabitethernet0    2       v2/D    1      UP
2.0.0.1      gigabitethernet1    0       v2/D    0      UP

Device2#show ip pim dense-mode neighbor
PIM Dense-mode Neighbor Table:
PIM Dense-mode VRF Name: Default
Total 1 Neighbor entries

Neighbor-Address Interface        Uptime/Expires    Ver
1.0.0.1      gigabitethernet0   00:12:39/00:01:35 v2
```

#We can see that the PIM-DM neighbor is set up between Device2 and Device1 successfully.

#View the IGMP information of the interface gigabitethernet1 on Device2.

```
Device2#show ip igmp interface gigabitethernet 1
Interface gigabitethernet1 (Index 5)
 IGMP Active, Querier (2.0.0.1)
 Default version 2
 IP router alert option in IGMP V2 msgs: EXCLUDE
 Internet address is 2.0.0.1
 IGMP query interval is 125 seconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1 seconds
 Last member query count is 2
 Group Membership interval is 260 seconds
 IGMP robustness variable is 2
```

**Step 4:** Configure C-BSR and C-RP.

#Configure Device1.

Configure interface gigabitethernet0 of Device1 as C-BSR and C-RP and the multicast group range of the C-RP service is 225.0.0.0/8.

```
Device1(config)#ip pim bsr-candidate gigabitethernet0
Device1(config)#ip access-list standard 1
```

```
Device1(config-std-nacl)#permit 225.0.0.0 0.255.255.255
Device1(config-std-nacl)#exit
Device1(config)#ip pim rp-candidate gigabitethernet0 group-list 1
```

#View the BSR and RP information of Device2.

```
Device2#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
  BSR address: 192.168.1.254
  BSR Priority: 0
  Hash mask length: 10
  Up time: 00:00:48
  Expiry time: 00:01:30
  Role: Non-candidate BSR
  State: Accept Preferred

Device2#show ip pim rp mapping
PIM Group-to-RP Mappings Table:
PIM VRF Name: Default
Total 1 RP set entry
Total 1 RP entry

  Group(s): 225.0.0.0/8
  RP count: 1
    RP: 192.168.1.254
      Info source: 192.168.1.254, via bootstrap, priority 192
      Up time: 00:00:42
      Expiry time: 00:01:48
```

#We can see that there is the BSR and RP information on Device2 and the multicast group range of the RP service is 225.0.0.0/8.

**Step 5:** Check the result.

#Receiver sends the IMGPv2 member relation report to add to multicast group 225.1.1.1, 226.1.1.1.

# Source sends the multicast packets with multicast group 225.1.1.1 and 226.1.1.1.

#View the multicast member table of Device2.

```
Device2#show ip igmp groups
IGMP Connected Group Membership
Total 2 groups
```

```
Group Address    Interface         Uptime   Expires  Last Reporter   V1 Expires
225.1.1.1        gigabitethernet1  02:28:52 00:02:26 2.0.0.2         stopped
226.1.1.1        gigabitethernet1  02:26:57 00:02:24 2.0.0.2         stopped
```

#View the PIM-SM multicast route table of Device1.

```
Device1#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(*, 225.1.1.1)
Up time: 02:23:32
RP: 192.168.1.254
RPF nbr: 0.0.0.0
RPF idx: None
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    gigabitethernet1  02:23:32/00:03:00
  Asserted interface list:


(192.168.1.1, 225.1.1.1)
Up time: 00:02:25
KAT time: 00:03:00
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: TRUE
Flags:
  JOIN DESIRED
```

```
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    gigabitethernet1  00:02:25/00:03:05
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 4324131

(192.168.1.1, 225.1.1.1, rpt)
Up time: 00:02:25
RP: 192.168.1.254
Flags:
  RPT JOIN DESIRED
  RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    gigabitethernet1
```

#View the PIM-DM multicast route table of Device1.

```
Device1#show ip pim dense-mode mroute
PIM-DM Multicast Routing Table
Total 1 mroute entry
(192.168.1.1, 226.1.1.1)
  Expire in: 00:02:46
  Source directly connected on gigabitethernet0
  State-Refresh Originator State: Originator
  Upstream IF: gigabitethernet0
    Upstream State: Forwarding
    Assert State: NoInfo
  Downstream IF List:
    gigabitethernet1, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```

#Receiver can receive the multicast service packets with multicast group 225.1.1.1. 226.1.1.1 sent by Source, and the multicast service packet with multicast group 225.1.1.1 uses PIM-SM to communicate; the multicast service packet with multicast group 226.1.1.1 uses PIM-DM to communicate.

**Note:**

- The viewing method of Device2 is the same as that of Device1, so the viewing process is omitted.

# 7. MVPN

## 7.1. Overview

With the promotion of the BGP/MPLS VPN service, the user puts forward the requirement of developing the multicast service in the VPN (Virtual Private Network) network and MVPN (Multicast Virtual Private Network) comes into being.

Similar to the unicast VPN, MVPN realizes the access and isolation of different MVPN users via the VRF mechanism. The MVPN users belonging to the same multicast domain can perform the multicast communication and the users of different multicast domains are isolated from each other.

The typical application environment: In the SP (Service Provider) network, run the PIM multicast routing protocol and run MVPN on the PE (Provider Edge). In the C (Client) network, also run the PIM multicast routing protocol. Each multicast domain sets up the Default MDT (Default Multicast Distribution Tree) in the SP network. The MVPN users of the same multicast domain are all added to one default MDT. The MVPN user receives the multicast data packets of the other MVPN users in the multicast domain via it.

There is one drawback to use Default MDT. Even PE does not have receiver, it also receives the multicast data packets sent by other PEs to Default MDT and then drop the packets. This causes the waste for the SP network bandwidth. To solve the problem, we can use the mode of setting up the Data MDT (Data Multicast Distribution Tree). The PE connected to the MVPN multicast source creates Data MDT according to the configuration rule to transmit the multicast data packets. Only the PEs with the receivers can be added to the corresponding Data MDT.

PE uses the address of Default MDT or Data MDT to encapsulate the multicast data packets of C network to the multicast data packet of the SP network and forward to the other PEs via the multicast distribution tree of the SP network. When PE has the receiver, de-capsulate the received multicast data packet and forward via the multicast distribution tree of the C network.

## 7.2. MVPN Function Configuration

Table 7-1 MVPN function configuration list

| Configuration Task | |
|---|---|
| Configure the MVPN basic functions | Configure the default multicast distribution tree. |
| | Configure the data multicast distribution tree. |
| Configure the RPF proxy | Configure the RPF proxy |
| Configure BGP MDT | Configure the BGP MDT address stack |

### 7.2.1. Configure MVPN Basic Functions

#### Configuration Conditions

Before configuring MVPN, first complete the following task:

- Configure MPLS L3VPN so that the users of the same VPN can perform the unicast communication normally;
- Configure the PIM-SM (or SSM) globally and in VPN;
- Enable the IP multicast route forwarding globally and in VPN.

### Configure Default MDT

After configuring Default MDT, the system automatically generates MTI and adds to Default MDT Group automatically.

Table 7-2 Configure the default MDT

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Enter the VRF instance configuration mode | **ip vrf** *vrf-name* | - |
| Enter the VRF IPv4 address family | **address-family ipv4** | - |
| Configure the default multicast distribution tree | **mdt default** *group-ip-address* | Mandatory<br>By default, do not configure the default MDT. |

**Caution:**

- Default MDTs of the same VPN in one network needs to be configured as one multicast group.

### Configure Data MDT

Set the switching threshold on the PE of the multicast source. When the PE finds that the forwarding rate of the multicast service packets reaches the threshold, create one MDT and only the PE of the receiver of the corresponding multicast group can be added to the new tree. After the switching is complete, the multicast service packets are not forwarded in Default MDT, but forwarded along Data MDT. This can prevent all multicast data from being forwarded along Default MDT, because not all PEs have the receivers of the multicast data.

Table 7-3 Configure the data MDT

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Enter the VRF instance configuration mode | **ip vrf** *vrf-name* | - |
| Enter the VRF IPv4 address family | **address-family ipv4** | - |
| Configure the MDT | **mdt data** *group-ip-address wildcard-mask* [ **threshold** *traffic-rate* ] [ **list** { *access-list-number* \| *access-list-name* } ] | Mandatory<br>By default, do not configure the data MDT. |

## 7.2.2. Configure RPF Proxy

### Configuration Condition

Before configuring the RPF proxy, first complete the following tasks:

- Configure MPLS L3VPN so that the users of the same VPN can perform the unicast communication normally;
- Configure the PIM-SM (or SSM) globally and in VPN;
- Enable the IP multicast route forwarding globally and in VPN;
- Configure MDT Default in VPN.

### Configure RPF Proxy

In the common MVPN environment, we need to specify the source IP and the next-hop address to the source IP in the PIM add packet sent by the PE device. In the Options-B across-domain scheme, do not perform the switching of the internal route between the autonomous domains, which will result in the failure of the RPF check of the P device for the PIM add packet from the PE device. To solve the problem, bring in the RPF proxy. After the PE device is configured with the RPF proxy, the PIM add packet sent by the PE device to the P device will contain the information of the RPF proxy. After the P device receives the PIM add packet containing the proxy message and finds that there is no route to the multicast source, query the next hop to the specified IP (in the autonomous domain, ASBR sets up the interface IP of the BGP neighbor with the peer ASBR) address in the proxy information to perform the RPF check.

Table 7-4 Configure the RPF proxy

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Configure the RPF proxy | **ip multicast rpf proxy rd vector vrf** *vrf-name* | Mandatory<br>By default, does not enable the RD vector proxy function of the multicast RPF. |

## 7.2.3. Configure BGP MDT Address Stack

### Configuration Condition

Before configuring the BGP MDT address stack, first complete the following tasks:

- Configure MPLS L3VPN so that the users of the same VPN can perform the unicast communication normally;
- Configure the PIM-SM (or SSM) globally and in VPN;
- Enable the IP multicast route forwarding globally and in VPN;
- Configure MDT Default in VPN.

### Configure BGP MDT Address Stack

Configure the BGP MDT address stack so that the BGP MDT route information can carry the local MTI address, Default MDT address and Data MDT address to advertise to the peer PE, so as to set up the source tree with the local MTI interface address as the source.

Table 7-5 Configure the BGP MDT address stack

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Enable the BGP protocol and enter the BGP configuration mode | **router bgp** *autonomous-system* | - |
| Configure the BGP neighbor | **neighbor** { *neighbor-address* \| *peer-group-name* } **remote-as** *as-number* | Mandatory<br>By default, do not create any BGP neighbor. |
| Configure the source address of the neighbor TCP session | **neighbor** { *neighbor-address* \| *peer-group-name* } **update-** | Mandatory<br>By default, the source address automatically adopts |

| Step | Command | Description |
|---|---|---|
| | **source** { *interface-name* \| *ip-address* } | the egress interface of the packet as the source address via the route selection. |
| Enter the BGP MDT address stack | **address-family ipv4 mdt** | - |
| Activate the capability of the BGP neighbor receiving and sending the MDT route | **neighbor** { *neighbor-address* \| *peer-group-name* } **activate** | Mandatory<br>By default, do not activate the capability of the BGP neighbor receiving and sending the MDT route. |

### 7.2.4. MVPN Monitoring and Maintaining

Table 7-6 MVPN monitoring and maintaining

| Command | Description |
|---|---|
| **show ip bgp ipv4 mdt** { **all** [ **summary** \| *ip-address* ] ] } \| **vrf** *vrf-name* [ *ip-address* ] \| **rd** *route-distinguisher* [ *ip-address* ] } | Display the BGP MDT route information |
| **show ip pim mdt** | Display the MDT information |
| **show ip pim mdt bgp** | Display the received BGP MDT SAFI information |
| **show ip pim mdt receive vrf** *vrf-name* | Display the received Data MDT information in VRF |
| **show ip pim mdt send vrf** *vrf-name* | Display the sent Data MDT information in VRF |
| **show ip pim mroute proxy** [ **vrf** *vrf-name* ] | Display the multicast RPF proxy information |

## 7.3. MVPN Typical Configuration Example

### 7.3.1. MVPN Typical Configuration in Single AS

#### Network Requirements

- Configure VPN instance 1 and configure the multicast Default MDT and Data MDT.

- Set up the MPLS L3VPN environment in the domain; enable the MPLS and BGP process on the PE; enable MPLS on the P;
- To enable the multicast enabling on all devices, we need to enable multicast enabling globally and in VPN instance 1 on the PE;
- Connect PE to the CE interface and add to VPN instance 1; enable the multicast protocol in the global interfaces and the interfaces of VPN instance 1;
- Configure the RP and BSR globally and in VPN instance 1;
- Send the multicast service packets at the Source and receive the multicast service packets at the Receiver, completing the multicast forwarding.

**Network Topology**

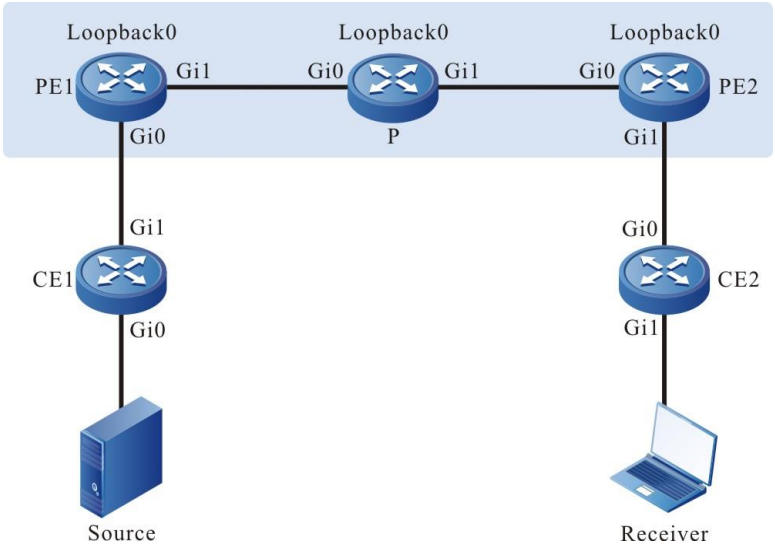


Figure 7-1 Networking of configuring MVPN in a single AS

| Device | Interface | IP address | Device | Interface | IP address |
|---|---|---|---|---|---|
| CE1 | Gi0 | 10.1.1.1/24 | P | Loopback0 | 172.0.0.3/32 |
| | Gi1 | 10.1.2.1/24 | PE2 | Gi0 | 192.168.2.2/24 |
| PE1 | Gi0 | 10.1.2.2/24 | | Gi1 | 10.2.1.1/24 |
| | Gi1 | 192.168.1.1/24 | | Loopback0 | 172.0.0.2/32 |
| | Loopback0 | 172.0.0.1/32 | CE2 | Gi0 | 10.2.1.2/24 |
| P | Gi0 | 192.168.1.2/24 | | Gi1 | 10.2.2.1/24 |
| | Gi1 | 192.168.2.1/24 | | | |

## Configuration Steps

**Step 1:** Configure the IP addresses of all device interfaces. (omitted)

**Step 2:** Configure the VPN instance on the PE.

#Configure PE1.

```
PE1#configure terminal
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
```

#Configure PE2.

```
PE2#configure terminal
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#exit
```

**Step 3:** Configure the VPN instance and IP address of the interface.

Take PE1 as an example:

```
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ip address 10.1.2.2 255.255.255.0
PE1(config-if-gigabitethernet0)#exit
```

**Note:**

- The configuration methods of VPN instance 1 interfaces of PE2 are similar;
- When configuring the interfaces of VPN instance 1 on the PE, first configure the interface to belong to VPF and then configure the IP address.

**Step 4:** Configure the backbone network IGP protocol to realize the unicast intercommunication of the backbone network.

#Configure OSPF on PE1.

```
PE1(config)#router ospf 200
PE1(config-ospf)#network 172.0.0.1 0.0.0.0 area 0
PE1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#Configure OSPF on PE2.

```
PE2(config)#router ospf 200
PE2(config-ospf)#network 172.0.0.2 0.0.0.0 area 0
PE2(config-ospf)#network 192.168.2.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#Configure OSPF on the P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 172.0.0.3 0.0.0.0 area 0
P(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
P(config-ospf)#network 192.168.2.0 0.0.0.255 area 0
P(config-ospf)#exit
```

#View the global route table of the device.

Take PE1 as an example:

```
PE1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   127.0.0.0/8 is directly connected, 04:48:06, lo0
C   192.168.1.0/24 is directly connected, 05:22:54, gigabitethernet1
O   192.168.2.0/24 [110/2] via 192.168.1.2, 02:23:57, gigabitethernet1
C   172.0.0.1/32 is directly connected, 05:17:37, loopback0
O   172.0.0.2/32 [110/3] via 192.168.1.2, 05:23:57, gigabitethernet1
O   172.0.0.3/32 [110/2] via 192.168.1.2, 05:27:47, gigabitethernet1
```

We can see that there are the loopback interface routes of PE2 and P in the route table of PE1.

**Note:**

- The checking method on PE2 and P is the same as that on PE1.

**Step 5:** Enable MPLS IP and MPLS LDP.

#Enable the global MPLS IP and MPLS LDP on PE1; enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 172.0.0.1
PE1(config-ldp)#transport-address 172.0.0.1
PE1(config-ldp)#exit
```

```
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#Enable the global MPLS IP and MPLS LDP on PE2; enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 172.0.0.2
PE2(config-ldp)#transport-address 172.0.0.2
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#Enable the global MPLS IP and MPLS LDP on P; enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 172.0.0.3
P(config-ldp)#transport-address 172.0.0.3
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#View the LDP session information on the device.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type     My Role   State        DeadTime
172.0.0.3          Multicast     Active    OPERATIONAL  00:02:34
Statistics for ldp sessions:
    Multicast sessions: 1
```

```
Targeted sessions: 0
```

We can see that PE1 and P set up the LDP session successfully.

**Note:**

- The checking method on PE2 and P is the same as that on PE1.

**Step 6:** Configure the IGP protocol in the VPN instance.

#Configure OSPF in the VPN instance on PE1.

```
PE1(config)#router ospf 100 vrf 1
PE1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#Configure OSPF in the VPN instance on PE2.

```
PE2(config)#router ospf 100 vrf 1
PE2(config-ospf)#network 10.2.1.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#Configure OSPF on CE1 and advertise the private network route.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
CE1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
CE1(config-ospf)#exit
```

#Configure OSPF on CE2 and advertise the private network route.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 10.2.1.0 0.0.0.255 area 0
CE2(config-ospf)#network 10.2.2.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

**Step 7:** Configure MP-IBGP, use the loopback interface as the peer address and perform the route re-distribution with the IGP protocol in the VPN instance.

#Configure MP-IBGP on PE1 and enable the VPNV4 address stack; perform the route re-distribution with the IGP protocol in the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 172.0.0.2 remote-as 100
PE1(config-bgp)#neighbor 172.0.0.2 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 172.0.0.2 activate
PE1(config-bgp-af)#neighbor 172.0.0.2 send-community both
```

```
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 100
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 100 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#Configure MP-IBGP on PE2 and enable the VPNV4 address stack; perform the route re-distribution with the IGP protocol in the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 172.0.0.1 remote-as 100
PE2(config-bgp)#neighbor 172.0.0.1 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 172.0.0.1 activate
PE2(config-bgp-af)#neighbor 172.0.0.1 send-community both
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 100
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 100 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

#View the BGP neighbor information on the PE.

Take PE1 as an example.

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 172.0.0.1, local AS number 100
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.0.0.2       4   100      40      41        5    0    0 00:32:01        2

Total number of neighbors 1
```

The content of the State/PfxRcd list is displayed as numbers (the number of the route prefixes received from the neighbor), indicating that PE1 and PE2 set up the BGP neighbor successfully.

#View the BGP VPNV4 route table and VPN route table on the PE.

Take PE1 as an example.

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 22, local router ID is 172.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[0]*> 10.1.1.0/24       10.1.2.1              2         32768 ?
[0]*> 10.1.2.0/24       0.0.0.0               1         32768 ?
[B]*>i10.2.1.0/24       172.0.0.2             1    100      0 ?
[B]*>i10.2.2.0/24       172.0.0.2             2    100      0 ?

PE1#show ip route vrf 1
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
     D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   10.1.1.0/24 [110/2] via 10.1.2.1, 46:02:56, gigabitethernet0
C   10.1.2.0/24 is directly connected, 148:00:45, gigabitethernet0
B   10.2.1.0/24 [200/1] via 172.0.0.2, 22:50:24, gigabitethernet1
B   10.2.2.0/24 [200/2] via 172.0.0.2, 22:50:24, gigabitethernet1
```

We can see that the BGP VPNV4 route table and VPN route table of PE1 both have the routes to CE2.

**Note:**

- The checking method on PE2 is the same as that on PE1.

#Check the route intercommunication.

```
CE1#ping 10.2.2.1

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 10.2.2.1 , timeout is 2 seconds:
```

```
!!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

We can see that CE1 can ping the route of CE2 successfully.

**Step 8:** Configure the backbone network and VPN instance multicast; configure BSR and RP.

#Enable the global multicast enabling on PE1 and multicast enabling in the VPN instance; enable the multicast protocol globally and on the VPN instance interface.

```
PE1(config)#ip multicast-routing
PE1(config)#ip multicast-routing vrf 1
PE1(config)#interface loopback0
PE1(config-if-loopback0)#ip pim sparse-mode
PE1(config-if-loopback0)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip pim sparse-mode
PE1(config-if-gigabitethernet0)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#ip pim sparse-mode
PE1(config-if-gigabitethernet1)#exit
```

#Enable the global multicast enabling on PE2 and multicast enabling in the VPN instance; enable the multicast protocol globally and on the VPN instance interface.

```
PE2(config)#ip multicast-routing
PE2(config)#ip multicast-routing vrf 1
PE2(config)#interface loopback0
PE2(config-if-loopback0)#ip pim sparse-mode
PE2(config-if-loopback0)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#ip pim sparse-mode
PE2(config-if-gigabitethernet0)#exit
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip pim sparse-mode
PE2(config-if-gigabitethernet1)#exit
```

#Enable the global multicast enabling on the P; enable the multicast protocol on the global interfaces and configure the global RP and BSR.

```
P(config)#ip multicast-routing
P(config)#interface loopback0
P(config-if-loopback0)#ip pim sparse-mode
P(config-if-loopback0)#exit
P(config)#interface gigabitethernet0
```

```
P(config-if-gigabitethernet0)#ip pim sparse-mode
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#ip pim sparse-mode
P(config-if-gigabitethernet1)#exit
P(config)#ip pim bsr-candidate loopback0
P(config)#ip pim rp-candidate loopback0
```

#Enable the multicast enabling on CE1 and enable the multicast protocol on the interface.

```
CE1(config)#ip multicast-routing
CE1(config)#interface gigabitethernet0
CE1(config-if-gigabitethernet0)#ip pim sparse-mode
CE1(config-if-gigabitethernet0)#exit
CE1(config)#interface gigabitethernet1
CE1(config-if-gigabitethernet1)#ip pim sparse-mode
CE1(config-if-gigabitethernet1)#exit
```

#Enable the multicast enabling on CE2; enable the multicast protocol on the interface; configure the RP and BSR of the VPN instance.

```
CE2(config)#ip multicast-routing
CE2(config)#interface gigabitethernet0
CE2(config-if-gigabitethernet0)#ip pim sparse-mode
CE2(config-if-gigabitethernet0)#exit
CE2(config)#interface gigabitethernet1
CE2(config-if-gigabitethernet1)#ip pim sparse-mode
CE2(config-if-gigabitethernet1)#exit
CE2(config)#ip pim bsr-candidate gigabitethernet0
CE2(config)#ip pim rp-candidate gigabitethernet0
```

**Step 9:** Configure Default MDT and Data MDT; after the configuration is complete, send the multicast packets of multicast group 225.0.0.1 and 225.0.0.2 on the Source and make Receiver to add to the multicast group 225.0.0.1 and 225.0.0.2.

#Configure Default MDT and Data MDT on PE1.

```
PE1(config)#ip vrf 1
PE1(config)#address-family ipv4
PE1(config-vrf-ipv4)#mdt default 239.1.1.1
PE1(config-vrf-ipv4)#mdt data 238.1.1.0 0.0.0.255
PE1(config-vrf-ipv4)#exit
```

#Configure Default MDT and Data MDT on PE2.

```
PE2(config)#ip vrf 1
PE2(config)#address-family ipv4
PE2(config-vrf-ipv4)#mdt default 239.1.1.1
PE2(config-vrf-ipv4)#mdt data 238.1.1.0 0.0.0.255
PE2(config-vrf-ipv4)#exit
```

**Step 10:** Check the result.

#View the multicast interface and MTI interface information of the VPN instance on the PE.

Take PE1 as an example.

```
PE1#show ip pim interface vrf 1
PIM Interface Table:
PIM VRF Name: 1
Total 2 Interface entries
Total 1 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address      Interface      VIF   Ver/  VIF  Nbr   DR      DR          BSR  CISCO
Neighbor
                            Index  Mode  Flag Count Priority          Border Neighbor
Filter
10.1.2.2     gigabitethernet0  0     v2/S  UP   1     1       10.1.2.2     FALSE
FALSE
172.0.0.1    tunnel1023     2     v2/S  UP   1     1       172.0.0.2    FALSE FALSE
```

We can see that there is the MTI interface information in the multicast interface of the VPN instance of PE1 and the MTI interface automatically gets the IP address. The address is the same as the IP address of the Loopback interface specified when configuring the BGP peer.

#View the neighbor information in the VPN instance on PE1.

Take PE1 as an example.

```
PE1#show ip pim neighbor vrf 1
PIM Neighbor Table:
PIM VRF Name: 1
Total 2 Neighbor entries

Neighbor      Interface      Uptime/Expires   Ver  DR
Address                                       Priority/Mode
10.1.2.1      gigabitethernet0  6d05h58m/00:01:36 v2   1 /
172.0.0.2     tunnel1023     00:01:28/00:01:17 v2   1 / DR
```

We can see that the MTI interface neighbor of PE1 is set up; we can see the MTI interface information of PE2 in the neighbor list.

**Note:**

- tunnel 1023 is the MTI interface of MVPN. The MTI interface is one interface of connecting VPN to the backbone multicast domain. It can be regarded as one channel connecting the VPN and the global. Each VPN creates one tunnel interface. When BGP enables the VPN address stack and Update-Source, Default MDT is configured in the VPN and there is multicast interface, the interface is generated automatically.

#View the Default MDT information on the PE.

Take PE1 as an example.

```
PE1#show ip pim mdt
Total 1 MDT Groups
 MDT Group      Interface      Source             VRF
 239.1.1.1      tunnel1023     loopback0          1
```

We can see that the MTI interface is added to Default MDT multicast group.

**Note:**

- The checking method on PE2 is the same as that on PE1.

#At the Source, send the multicast flow of multicast group 225.0.0.1 and 225.0.0.2; at the Receiver, receive multicast group 225.0.0.1 and 225.0.0.2; when there is multicast traffic, view the Group in the backbone network on PE2.

```
PE2#show ip igmp groups
IGMP Static Group Membership
Total 6 static groups
Group Address   Source Address   Interface
239.1.1.1       0.0.0.0          loopback0
239.1.1.1       172.0.0.1        loopback0
238.1.1.0       0.0.0.0          loopback0
238.1.1.0       172.0.0.1        loopback0
238.1.1.1       0.0.0.0          loopback0
238.1.1.1       172.0.0.1        loopback0
```

We can see that the loopback port is automatically added to Default MDT multicast group. When there is multicast traffic, we can see that the loopback port of PE2 is automatically added to Data MDT multicast group and the backbone network is switched from Default MDT to Data-MDT.

#View the Data MDT switching information on the PE.

```
PE1#show ip pim mdt send vrf 1
MDT-data send list for VRF: 1
Total 2 MDT-data Groups
 (source, group)              MDT-data group     ref_count
 (10.1.1.2, 225.0.0.2)        238.1.1.1          1
```

```
(10.1.1.2, 225.0.0.1)          238.1.1.0          1
```

```
PE2#show ip pim mdt receive vrf 1
Joined MDT-data [group : source] for VRF: 1
Total 2 MDT-data Groups
 [238.1.1.0 : 172.0.0.1]
 [238.1.1.1 : 172.0.0.1]
```

We can see that PE1 sends the Data MDT switching information and PE2 also receives the Data MDT switching information of PE1 successfully.

## 7.3.2. Across-AS MVPN Typical Configuration

### Network Requirements

- Configure VPN instance 1 on the PE and configure the multicast Default MDT and Data MDT.
- Set up the OptionB across-domain MPLS L3VPN environment; enable the MPLS and BGP process on the PE and ASBR;
- To enable the multicast enabling on all devices, we need to enable multicast enabling globally and in VPN instance 1 on the PE;
- Connect PE to the CE interface and add to VPN instance 1; enable the multicast protocol in the global interfaces and the interfaces of VPN instance 1;
- Enable SSM on the devices except for the CE devices, associate all multicast group addresses, and configure the RP and BSR of VPN instance 1 on the CE;
- Send the multicast flow at the Source and receive the multicast flow at the Receiver, completing the multicast forwarding.

### Network Topology

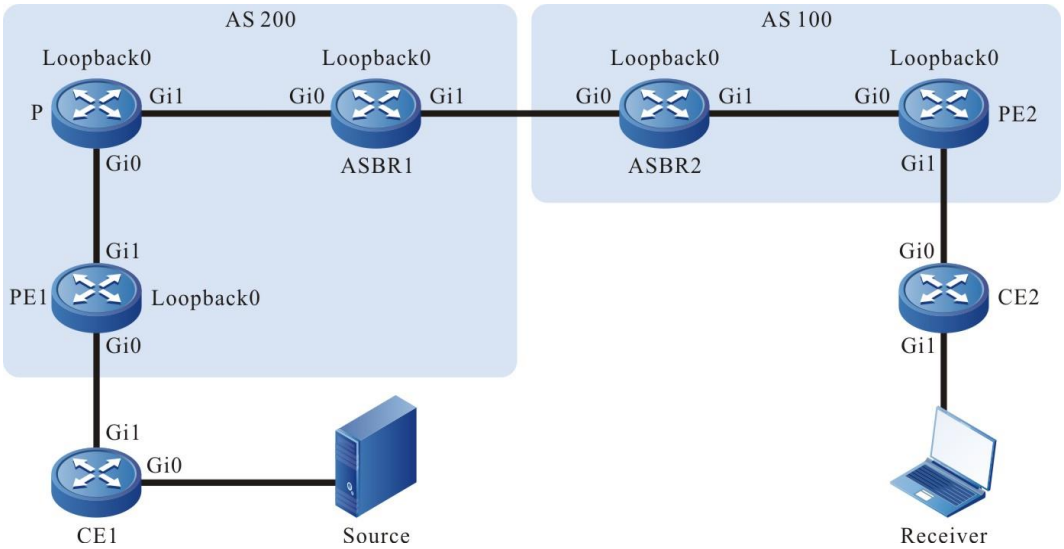


Figure 7-2 Networking of configuring MVPN across-AS

| Device | Interface | IP address | Device | Interface | IP address |
|---|---|---|---|---|---|
| CE1 | Gi0 | 10.1.2.1/24 | ASBR1 | Loopback0 | 172.0.0.2/32 |
| | Gi1 | 10.1.1.2/24 | ASBR2 | Gi0 | 192.168.3.2/24 |
| PE1 | Gi0 | 10.1.1.1/24 | | Gi1 | 100.1.1.1/24 |
| | Gi1 | 192.168.1.1/24 | | Loopback0 | 172.0.0.3/32 |
| | Loopback0 | 172.0.0.1/32 | PE2 | Gi0 | 100.1.1.2/24 |
| P | Gi0 | 192.168.1.2/24 | | Gi1 | 11.1.1.1/24 |
| | Gi1 | 192.168.2.1/24 | | Loopback0 | 172.0.0.4/32 |
| | Loopback0 | 172.0.0.5/32 | CE2 | Gi0 | 11.1.1.2/24 |
| ASBR1 | Gi0 | 192.168.2.2/24 | | Gi1 | 11.1.2.1/24 |
| | Gi1 | 192.168.3.1/24 | | | |

## Configuration Steps

**Step 1:** Configure the IP addresses of all device interfaces. (omitted)

**Step 2:** Create the VPN instance on the PE.

#Configure PE1.

```
PE1#configure terminal
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
```

#Configure PE2.

```
PE1#configure terminal
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
```

```
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#exit
```

**Step 3:** Configure the belonging VPN instance and IP address of the interface.

**Note:**

- When configuring the interface of VPN instance 1 on the PE, first configure the interface to belong to VPF and then configure the IP address.

Take PE1 as an example.

```
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip vrf forwarding 1
PE1(config-if-gigabitethernet0)#ip address 10.1.1.1 255.255.255.0
PE1(config-if-gigabitethernet0)#exit
```

**Note:**

- The checking method on PE2 is the same as that on PE1.

**Step 4:** Configure the backbone network and OSPF in the VPN instance.

#Configure the OSPF on PE1 globally and in the VPN instance.

```
PE1(config)#router ospf 100
PE1(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
PE1(config-ospf)#network 172.0.0.1 0.0.0.0 area 0
PE1(config-ospf)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
PE1(config-ospf)#exit
```

#Configure the OSPF globally on the P.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 192.168.1.0 0.0.0.255 area 0
P(config-ospf)#network 172.0.0.5 0.0.0.0 area 0
P(config-ospf)#network 192.168.2.0 0.0.0.255 area 0
P(config-ospf)#exit
```

#Configure the OSPF globally on the ASBR1.

```
ASBR1#configure terminal
ASBR1(config)#router ospf 100
ASBR1(config-ospf)#network 192.168.2.0 0.0.0.255 area 0
ASBR1(config-ospf)#network 172.0.0.2 0.0.0.255 area 0
ASBR1(config-ospf)#exit
```

#Configure the OSPF globally on the ASBR2.

```
ASBR2#configure terminal
ASBR2(config)#router ospf 100
ASBR2(config-ospf)#network 100.1.1.0 0.0.0.255 area 0
ASBR2(config-ospf)#network 172.0.0.3 0.0.0.255 area 0
ASBR2(config-ospf)#exit
```

#Configure the OSPF globally on PE2 and in the VPN instance.

```
PE2(config)#router ospf 100
PE2(config-ospf)#network 100.1.1.0 0.0.0.255 area 0
PE2(config-ospf)#network 172.0.0.4 0.0.0.0 area 0
PE2(config-ospf)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 11.1.1.0 0.0.0.255 area 0
PE2(config-ospf)#exit
```

#Configure the OSPF globally on the CE1.

```
CE1#configure terminal
CE1(config)#router ospf 100
CE1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
CE1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
CE1(config-ospf)#exit
```

# Configure the OSPF globally on the CE2.

```
CE2#configure terminal
CE2(config)#router ospf 100
CE2(config-ospf)#network 11.1.1.0 0.0.0.255 area 0
CE2(config-ospf)#network 11.1.2.0 0.0.0.255 area 0
CE2(config-ospf)#exit
```

#View the global route table on the device.

Take PE2 as an example.

```
PE2#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   100.1.1.0/24 is directly connected, 06:38:51, gigabitethernet1
C   127.0.0.0/8 is directly connected, 513:34:42, lo0
```

O 172.0.0.3/32 [110/2] via 100.1.1.1, 04:31:09, gigabitethernet1

C 172.0.0.4/32 is directly connected, 83:48:24, loopback0

We can see that there is the information of the route to the ASBR2 loopback port in the global route table of PE2.

**Note:**

- The checking method on PE1 and ASBR is the same as that on PE2.

**Step 5:** Enable MPLS IP and MPLS LDP.

#Enable the global MPLS IP and MPLS LDP on the PE1; enable MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 172.0.0.1
PE1(config-ldp)#transport-address 172.0.0.1
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#mpls ip
PE1(config-if-gigabitethernet1)#mpls ldp
PE1(config-if-gigabitethernet1)#exit
```

#Enable the global MPLS IP and MPLS LDP on the P; enable MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 172.0.0.5
P(config-ldp)#transport-address 172.0.0.5
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#Enable the global MPLS IP and MPLS LDP on the ASBR1; enable MPLS IP and MPLS LDP on the interface.

```
ASBR1(config)#mpls ip
ASBR1(config)#mpls ldp
```

```
ASBR1(config-ldp)#router-id 172.0.0.2
ASBR1(config-ldp)#transport-address 172.0.0.2
ASBR1(config-ldp)#exit
ASBR1(config)#interface gigabitethernet0
ASBR1(config-if-gigabitethernet0)#mpls ip
ASBR1(config-if-gigabitethernet0)#mpls ldp
ASBR1(config-if-gigabitethernet0)#exit
ASBR1(config)#interface gigabitethernet1
ASBR1(config-if-gigabitethernet1)#mpls ip
ASBR1(config-if-gigabitethernet1)#exit
```

#Enable the global MPLS IP and MPLS LDP on the ASBR2; enable MPLS IP and MPLS LDP on the interface.

```
ASBR2(config)#mpls ip
ASBR2(config)#mpls ldp
ASBR2(config-ldp)#router-id 172.0.0.3
ASBR2(config-ldp)#transport-address 172.0.0.3
ASBR2(config-ldp)#exit
ASBR2(config)#interface gigabitethernet0
ASBR2(config-if-gigabitethernet0)#mpls ip
ASBR2(config-if-gigabitethernet0)#exit
ASBR2(config)#interface gigabitethernet1
ASBR2(config-if-gigabitethernet1)#mpls ip
ASBR2(config-if-gigabitethernet1)#mpls ldp
ASBR2(config-if-gigabitethernet1)#exit
```

#Enable the global MPLS IP and MPLS LDP on the PE2; enable MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 172.0.0.4
PE2(config-ldp)#transport-address 172.0.0.4
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#View the LDP session information on the device.

Take P as an example.

```
P#show mpls ldp session
Peer IP Address    Peer Type     My Role   State        DeadTime
172.0.0.1          Multicast     Active    OPERATIONAL  00:02:58
172.0.0.2          Multicast     Active    OPERATIONAL  00:02:48
Statistics for ldp sessions:
    Multicast sessions: 2
    Targeted sessions: 0
```

We can see that P sets up the LDP session with PE1 and ASBR1 successfully.

**Note:**

- The checking method on ASBR and PE is the same as that on the P device.

**Step 6:** Configure MP-IBGP between PE and ASBR, use the loopback interface as the peer address, configure MP-EBGP between ASBRs, and perform the route re-distribution with the IGP protocol in the VPN instance.

#Configure MP-IBGP on PE1, enable the VPNV4 address stack and MDT address stack, and perform the route re-distribution with the IGP protocol in the VPN instance.

```
PE1(config)#router bgp 200
PE1(config-bgp)#neighbor 172.0.0.2 remote-as 200
PE1(config-bgp)#neighbor 172.0.0.2 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 172.0.0.2 activate
PE1(config-bgp-af)#neighbor 172.0.0.2 send-community extended
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 mdt
PE1(config-bgp-af)#neighbor 172.0.0.2 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 200
PE1(config-ospf)#exit
```

#Configure MP-IBGP with PE1 on ASBR1, configure MP-EBGP between ASBR1 and ASBR2, and enable VPNV4 address stack and MDT address stack.

```
ASBR1(config)#router bgp 200
ASBR1(config-bgp)#neighbor 172.0.0.1 remote-as 200
ASBR1(config-bgp)#neighbor 172.0.0.1 update-source loopback0
ASBR1(config-bgp)#neighbor 192.168.3.2 remote-as 100
```

```
ASBR1(config-bgp)#address-family vpnv4
ASBR1(config-bgp-af)#neighbor 172.0.0.1 activate
ASBR1(config-bgp-af)#neighbor 172.0.0.1 next-hop-self
ASBR1(config-bgp-af)#neighbor 172.0.0.1 send-community extended
ASBR1(config-bgp-af)#neighbor 192.168.3.2 activate
ASBR1(config-bgp-af)#neighbor 192.168.3.2 send-community extended
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#address-family ipv4 mdt
ASBR1(config-bgp-af)#neighbor 172.0.0.1 activate
ASBR1(config-bgp-af)#neighbor 172.0.0.1 next-hop-self
ASBR1(config-bgp-af)#neighbor 192.168.3.2 activate
ASBR1(config-bgp-af)#exit-address-family
ASBR1(config-bgp)#exit
```

#Configure MP-IBGP with PE2 on ASBR2, configure MP-EBGP between ASBR2 and ASBR1, and enable VPNV4 address stack and MDT address stack.

```
ASBR2(config)#router bgp 100
ASBR2(config-bgp)#neighbor 172.0.0.4 remote-as 100
ASBR2(config-bgp)#neighbor 172.0.0.4 update-source loopback0
ASBR2(config-bgp)#neighbor 192.168.3.1 remote-as 200
ASBR2(config-bgp)#address-family vpnv4
ASBR2(config-bgp-af)#neighbor 172.0.0.4 activate
ASBR2(config-bgp-af)#neighbor 172.0.0.4 next-hop-self
ASBR2(config-bgp-af)#neighbor 172.0.0.4 send-community extended
ASBR2(config-bgp-af)#neighbor 192.168.3.1 activate
ASBR2(config-bgp-af)#neighbor 192.168.3.1 send-community extended
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#address-family ipv4 mdt
ASBR2(config-bgp-af)#neighbor 172.0.0.4 activate
ASBR2(config-bgp-af)#neighbor 172.0.0.4 next-hop-self
ASBR2(config-bgp-af)#neighbor 192.168.3.1 activate
ASBR2(config-bgp-af)#exit-address-family
ASBR2(config-bgp)#exit
```

#Configure MP-IBGP on PE2, enable the VPNV4 address stack and MDT address stack, and perform the route re-distribution with the IGP protocol in the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 172.0.0.3 remote-as 100
PE2(config-bgp)#neighbor 172.0.0.3 update-source loopback0
PE2(config-bgp)#address-family vpnv4
```

```
PE2(config-bgp-af)#neighbor 172.0.0.3 activate
PE2(config-bgp-af)#neighbor 172.0.0.3 send-community extended
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 mdt
PE2(config-bgp-af)#neighbor 172.0.0.3 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

#View the BGP neighbor information on the device.

Take ASBR1 as an example.

```
ASBR1#show ip bgp vpnv4 all summary
BGP router identifier 172.0.0.2, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.0.0.1       4   200       2       2        1    0    0 00:00:14        2
192.168.3.2     4   100       7       8        1    0    0 00:05:28        2

Total number of neighbors 2
```

#The content of the State/PfxRcd list is displayed as numbers (the number of the route prefixes received from the neighbor), indicating that ASBR1 sets up the BGP neighbor with PE1 and ASBR2 successfully.

#View the BGP VPNV4 route table on the BGP device.

Take ASBR1 as an example.

```
ASBR1#show ip bgp vpnv4 all
BGP table version is 7, local router ID is 172.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1
```

```
[B]*>i10.1.1.0/24        172.0.0.1          1    100      0 ?
[B]*>i10.1.2.0/24        172.0.0.1          2    100      0 ?
[B]*> 11.1.1.0/24        192.168.3.2        0             0 100 ?
[B]*> 11.1.2.0/24        192.168.3.2        0             0 100 ?
```

We can see that there is the route to the local CE1 and the peer CE2 in the BGP VPNV4 of ASBR1.

**Note:**

- The checking method on PE and ASBR2 is the same as that on ASBR1.

**Step 7:** Configure the backbone network PIM domain to adopt the SSM mode; the VPN instance configures the multicast routing protocol PIM-SM; configure BSR and RP.

#Enable the multicasting enabling globally and of the VPN instance on PE1, the RPF proxy function in VPN and the global SSM; configure the multicast protocol on the interface.

```
PE1(config)#ip multicast-routing
PE1(config)#ip multicast-routing vrf 1
PE1(config)#ip multicast rpf proxy rd vector vrf 1
PE1(config)#interface loopback 0
PE1(config-if-loopback0)#ip pim sparse-mode
PE1(config-if-loopback0)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#ip pim sparse-mode
PE1(config-if-gigabitethernet0)#exit
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#ip pim sparse-mode
PE1(config-if-gigabitethernet1)#exit
PE1(config)#ip pim ssm default
```

#Enable the global multicast enabling and SSM function on the P; configure the multicast protocol on the interface.

```
P(config)#ip multicast-routing
P(config)#interface loopback 0
P(config-if-loopback0)#ip pim sparse-mode
P(config-if-loopback0)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#ip pim sparse-mode
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#ip pim sparse-mode
P(config-if-gigabitethernet1)#exit
P(config)#ip pim ssm default
```

#Enable the global multicast enabling and SSM function on ASBR1; configure the multicast protocol on the interface.

```
ASBR1(config)#ip multicast-routing
ASBR1(config)#interface loopback 0
ASBR1(config-if-loopback0)#ip pim sparse-mode
ASBR1(config-if-loopback0)#exit
ASBR1(config)#interface gigabitethernet0
ASBR1(config-if-gigabitethernet0)#ip pim sparse-mode
ASBR1(config-if-gigabitethernet0)#exit
ASBR1(config)#interface gigabitethernet1
ASBR1(config-if-gigabitethernet1)#ip pim sparse-mode
ASBR1(config-if-gigabitethernet1)#exit
ASBR1(config)#ip pim ssm default
```

#Enable the global multicast enabling and SSM function on ASBR2; configure the multicast protocol on the interface.

```
ASBR2(config)#ip multicast-routing
ASBR2(config)#interface loopback 0
ASBR2(config-if-loopback0)#ip pim sparse-mode
ASBR2(config-if-loopback0)#exit
ASBR2(config)#interface gigabitethernet0
ASBR2(config-if-gigabitethernet0)#ip pim sparse-mode
ASBR2(config-if-gigabitethernet0)#exit
ASBR2(config)#interface gigabitethernet1
ASBR2(config-if-gigabitethernet1)#ip pim sparse-mode
ASBR2(config-if-gigabitethernet1)#exit
ASBR2(config)#ip pim ssm default
```

#Enable the multicasting enabling globally and of the VPN instance on PE2, the RPF proxy function in VPN and the global SSM; configure the multicast protocol on the interface.

```
PE2(config)#ip multicast-routing
PE2(config)#ip multicast-routing vrf 1
PE2(config)#ip multicast rpf proxy rd vector vrf 1
PE2(config)#interface loopback 0
PE2(config-if-loopback0)#ip pim sparse-mode
PE2(config-if-loopback0)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#ip pim sparse-mode
PE2(config-if-gigabitethernet0)#exit
PE2(config)#interface gigabitethernet1
```

```
PE2(config-if-gigabitethernet1)#ip pim sparse-mode
PE2(config-if-gigabitethernet1)#exit
PE2(config)#ip pim ssm default
```

#Enable the global multicast enabling on CE1; configure the RP and BSR in the VPN instance; configure the multicast protocol on the interface.

```
CE1(config)#ip multicast-routing
CE1(config)#interface gigabitethernet0
CE1(config-if-gigabitethernet0)#ip pim sparse-mode
CE1(config-if-gigabitethernet0)#exit
CE1(config)#interface gigabitethernet1
CE1(config-if-gigabitethernet1)#ip pim sparse-mode
CE1(config-if-gigabitethernet1)#exit
CE1(config)#ip pim bsr-candidate gigabitethernet1
CE1(config)#ip pim rp-candidate gigabitethernet1
```

#Enable the global multicast enabling on CE2; configure the multicast protocol on the interface.

```
CE2(config)#ip multicast-routing
CE2(config)#interface gigabitethernet0
CE2(config-if-gigabitethernet0)#ip pim sparse-mode
CE2(config-if-gigabitethernet0)#exit
CE2(config)#interface gigabitethernet1
CE2(config-if-gigabitethernet1)#ip pim sparse-mode
CE2(config-if-gigabitethernet1)#exit
```

**Note:**

- Here, use the default range of SSM 232.0.0.0/8; the SSM range can use **ip pim ssm range** to change. The SSM range should contain Default MDT and Data MDT.

#View the global multicast interface information of the device in the backbone network.

Take PE1 as an example.

```
PE1#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 2 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address      Interface      VIF    Ver/  VIF  Nbr   DR      DR          BSR  CISCO
Neighbor
                            Index  Mode  Flag Count Priority            Border Neighbor
Filter
```

```
192.168.1.1     gigabitethernet1  2       v2/S  UP   1    1        192.168.1.2     FALSE
FALSE
172.0.0.1       loopback0         0       v2/S  UP   0    1        172.0.0.1       FALSE  FALSE
```

We can see that there is the loopback port and Gi1 in the global multicast interface information of PE1.

#View the global multicast neighbor information of the device in the backbone network.

Take PE1 as an example.

```
PE1#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 1 Neighbor entry

Neighbor        Interface        Uptime/Expires    Ver   DR
Address                                            Priority/Mode
192.168.1.2     gigabitethernet1  2d00h06m/00:01:36 v2    1 / DR
```

We can see that there is the interface address information of P in the global multicast neighbor information of PE1.

**Note:**

- The checking method on PE2 and ASBR is the same as that of PE1.

#View the RP and BSR information in the multicast VPN on the device.

Take PE1 and CE2 as an example.

```
PE1#show ip pim rp mapping vrf 1
PIM Group-to-RP Mappings Table:
PIM VRF Name: 1
Total 1 RP set entry
Total 1 RP entry

  Group(s): 224.0.0.0/4
  RP count: 1
    RP: 10.1.1.2
      Info source: 10.1.1.2, via bootstrap, priority 192
      Up time: 00:07:51
      Expiry time: 00:00:39

PE1#show ip pim bsr-router vrf 1
PIMv2 Bootstrap information
PIM VRF Name: 1
  BSR address: 10.1.1.2
```

```
  BSR Priority: 0
  Hash mask length: 10
  Up time: 00:08:47
  Expiry time: 00:00:14
  Role: Non-candidate BSR
  State: Accept Preferred

CE2#show ip pim rp mapping
PIM Group-to-RP Mappings Table:
PIM VRF Name: Default
Total 1 RP set entry
Total 1 RP entry

  Group(s): 224.0.0.0/4
  RP count: 1
    RP: 10.1.1.2
      Info source: 10.1.1.2, via bootstrap, priority 192
      Up time: 00:09:29
      Expiry time: 00:02:01

CE2#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
  BSR address: 10.1.1.2
  BSR Priority: 0
  Hash mask length: 10
  Up time: 00:10:18
  Expiry time: 00:01:43
  Role: Non-candidate BSR
  State: Accept Preferred
```

We can see that there is the BSR and RP information in the VPN of PE1 and the global of CE2.

**Note:**

- The checking method on PE2 and CE1 is the same as that on PE1 and CE2.

**Step 8:** Configure Default MDT and Data MDT.

#Configure Default MDT and Data MDT on PE1.

```
PE1(config)#ip vrf 1
```

```
PE1(config)#address-family ipv4
PE1(config-vrf-ipv4)#mdt default 232.0.0.1
PE1(config-vrf-ipv4)#mdt data 232.1.1.0 0.0.0.255
PE1(config-vrf-ipv4)#exit
```

#Configure Default MDT and Data MDT on PE2.

```
PE2(config)#ip vrf 1
PE2(config)#address-family ipv4
PE2(config-vrf-ipv4)#mdt default 232.0.0.1
PE2(config-vrf-ipv4)#mdt data 232.1.1.0 0.0.0.255
PE2(config-vrf-ipv4)#exit
```

**Step 9:** Check the result.

#View the BGP MDT route table on the device enabled with the BGP MDT address stack.

Take PE1 as an example.

```
PE1#show ip bgp ipv4 mdt all
BGP table version is 2, local router ID is 172.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop         Metric LocPrf Weight Path
Route Distinguisher: 100:1
[?]*> 172.0.0.1/32       0.0.0.0                       0 ?
[B]*>i172.0.0.4/32       172.0.0.2              0    100      0 100 ?
```

We can see that there is the information of the route to the MTI interface of PE2 in the BGP MDT route table of PE1.

#View the MTI interface information on the PE.

Take PE1 as an example.

```
PE1#show ip pim interface vrf 1
PIM Interface Table:
PIM VRF Name: 1
Total 2 Interface entries
Total 1 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address         Interface       VIF    Ver/  VIF  Nbr   DR      DR          BSR   CISCO
Neighbor
```

```
                                Index   Mode   Flag  Count  Priority          Border Neighbor
Filter
10.1.1.1      gigabitethernet0  0       v2/S   UP    1      1        10.1.1.2       FALSE  FALSE
172.0.0.1     tunnel1023        2       v2/S   UP    1      1        172.0.0.4      FALSE  FALSE
```

We can see that the multicast interface of the VPN instance of PE1 has tunnel1023 and the MTI interface automatically gets the IP address. The address is the same as the IP address of the loopback interface specified when configuring the BGP peer.

#View the multicast neighbor information in the VPN instance on the PE.

Take PE1 as an example.

```
PE1#show ip pim neighbor vrf 1
PIM Neighbor Table:
PIM VRF Name: 1
Total 2 Neighbor entries

Neighbor        Interface        Uptime/Expires    Ver   DR
Address                                            Priority/Mode
10.1.1.2        gigabitethernet0   6d05h58m/00:01:36  v2    1 / DR
172.0.0.4       tunnel1023         00:01:28/00:01:17  v2    1 / DR
```

We can see that the MTI neighbor of PE1 is set up and there is the information of the MTI interface of PE2 in the neighbor list.

**Note:**

- tunnel 1023 is the MTI interface of MVPN. The MTI interface is one interface of connecting VPN to the backbone multicast domain. It can be regarded as one channel connecting the VPN and the global. Each VPN creates one tunnel interface. When BGP enables the VPN address stack and Update-Source, Default MDT is configured in the VPN and there is multicast interface, the interface is generated automatically.

#View the Default MDT information on the PE.

Take PE1 as an example.

```
PE1#show ip pim mdt
Total 1 MDT Groups
  MDT Group       Interface        Source              VRF
  232.0.0.1       tunnel1023       loopback0           1
```

We can see that the MTI interface of PE1 is added to the Default MDT multicast group.

#View the global multicast route table on the device.

Take PE1 as an example.

```
PE1#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
```

```
Total 0 (*,G) entry
Total 4 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(172.0.0.1, 232.1.1.0)
Up time: 00:15:37
KAT time: 00:02:52
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    gigabitethernet1  00:15:37/00:02:53
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 743987

(172.0.0.1, 232.1.1.1)
Up time: 00:15:37
KAT time: 00:02:52
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    gigabitethernet1  00:15:37/00:02:53
  Asserted interface list:
```

```
  Outgoing interface list:
    gigabitethernet1
  Packet count 743847

(172.0.0.1, 232.0.0.1)
Up time: 00:41:16
KAT time: 00:02:52
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    gigabitethernet1  00:39:20/00:03:07
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 39840

(172.0.0.4, 232.0.0.1)
Up time: 00:39:07
KAT time: 00:02:52
RPF nbr: 192.168.1.2 Vector: 172.0.0.2
RPF idx: gigabitethernet1
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    loopback0
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    loopback0
  Packet count 144
```

The used by the backbone network is PIM-SSM, so we can see that there is no the (*, G) entry in the multicast route table of the PE1 backbone network and the RPF proxy takes effect. On PE1, we can see that the RPF neighbor 172.0.0.2 of the source address 172.0.0.4 is replaced to 192.168.1.2, so as to complete the setup of the across-domain Default MDT.

**Note:**

- The checking method of PE2 is the same as that of PE1

#At the Source, send the multicast flow of multicast group 225.0.0.1 and 225.0.0.2; at the Receiver, receive the multicast group 225.0.0.1 and 225.0.0.2; when there is multicast traffic, view the Group in the backbone network on PE2.

```
PE2#show ip igmp groups
IGMP Static Group Membership
Total 6 static groups
Group Address    Source Address   Interface
232.1.1.0        0.0.0.0          loopback0
232.1.1.0        172.0.0.1        loopback0
232.1.1.1        0.0.0.0          loopback0
232.1.1.1        172.0.0.1        loopback0
232.0.0.1        0.0.0.0          loopback0
232.0.0.1        172.0.0.1        loopback0
```

We can see that the loopback port of PE2 is automatically added to Default MDT multicast group. When there is multicast traffic, the loopback port of PE2 is automatically added to Data MDT multicast group and the backbone network is switched from Default Mdt to Data-MDT.

#View the Data-MDT switching information on the PE.

```
PE1#show ip pim mdt send vrf 1
MDT-data send list for VRF: 1
Total 2 MDT-data Groups
  (source, group)              MDT-data group     ref_count
  (10.1.2.2, 225.0.0.2)        232.1.1.1          1
  (10.1.2.2, 225.0.0.1)        232.1.1.0          1

PE2#show ip pim mdt receive vrf 1
Joined MDT-data [group : source] for VRF: 1
Total 2 MDT-data Groups
 [232.1.1.0 : 172.0.0.1]
 [232.1.1.1 : 172.0.0.1]
```

We can see that PE1 sends the switching information of Data MDT and PE2 also receives the Data MDT switching information of PE1 successfully.

# 8. NG MVPN

## 8.1. Overview

NG MVPN (Next Generation MVPN) is a new generation framework for IP multicast data traffic across BGP/MPLS VPN network. It provides BGP-based signaling transfer mode and PIM SM/PIM SSM/P2MP TE/mLDP and other data bearing modes, so that multicast and unicast services can be unified in the same VPN architecture.

BGP/MPLS IP VPN is widely used in the existing network because of its high reliability and security. IP multicast is also welcomed by service providers because of its efficient point-to-multipoint transmission mode. The development of IPTV, video conferencing, distance education and other services has put forward higher requirements for the reliability, security and efficiency of the network, so service providers have also generated more and more demands for running IP multicast services on BGP/MPLS IP VPN network. Multicast Virtual Private Network (MVPN) solution is produced under this background. With the MVPN technology, multicast services can be provisioned on existing BGP/MPLS IP VPN, and private multicast data traffic can be transmitted to the remote site of VPN through the public network. At present, the implementation of MVPN is based on RFC 6037 (draft-rosen-vpn-mcast-06), so it is also called Rosen MVPN. Rosen MVPN uses PIM protocol to establish a multicast distribution tree in both public and private networks to transmit private multicast protocol packets and multicast data traffic. Its shortcomings lie in: because private multicast protocol packets and data traffic need to be transmitted through the multicast distribution tree, the public network must enable multicast function. Otherwise, multicast distribution tree can not be established, which makes network deployment complex.

The public network uses GRE encapsulation to realize the transmission of the multicast data traffic, and cannot use some advantages of MPLS in the existing BGP/MPLS IP VPN network, such as reliability, TE bandwidth reservation and QoS guarantee.

NG MVPN has made some improvements relative to MVPN in Rosen mode. NG MVPN is characterized by:

The public network uses BGP to transmit private multicast protocol message and private multicast route, and does not need to configure other multicast protocols, simplifying the complexity of network deployment and reducing the difficulty of network maintenance.

The public network uses the mature tag forwarding technology and tunnel protection technology of MPLS to make multicast service quality higher and reliability better.

## 8.2. NG MVPN Function Configuration

Table 8-1 NG MVPN function configuration list

| Configuration tasks | |
|---|---|
| Configure NG MVPN basic functions | Configure MVPN ID |
| | Configure VRF attributes |
| | Configure a I-PMSI tunnel |
| | Configure S-PMSI tunnel switching |

| Configuration tasks | |
|---|---|
| Configure BGP MVPN | Configure BGP MVPN address family |
| Configure MVPN ORF | Configure the BGP MVPN address family to filter at the outgoing direction |

## 8.2.1. Configure NG MVPN Basic Functions

### Configuration Conditions

Before configuring NG MVPN, first complete the following tasks:

- Configure MPLS L3VPN so that the same VPN user can perform the unicast communication normally
- Configure PIM-SM (SSM) in VPN
- Enable the IP multicast route forwarding in VPN

### Configure MVPN ID

MVPN ID is used to identify one MVPN member. In one MVPN, MVPN ID is unique globally. Sender PE (Sender Provider Edge) and Receiver PE (Receiver Provider Edge) both need to be configure with the MVPN ID.

Table 8-2 Configure MVPN ID

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Configure MVPN ID | **mvpn-id** *ip-address* | Mandatory<br>By default, do not configure the MVPN ID. |

**Caution:**

- The configured MVPN ID should be the global reachable IPv4 address on the local device.

### Configure VRF Attributes

When the local PE receives MVPN routing information sent by the remote PE device, the local PE device needs to determine which local VRF to load the MVPN route. In order to control the distribution of MVPN routes, each VRF needs one or more MVPN RT attributes. MVPN RT attributes have two kinds: Export RT and Import RT. When PE initiates MVPN routing, it carries the Export RT attribute. When PE decides which VRF the MVPN route will be imported into, it uses the Export RT attribute carried by the route to match the Import RT of the local VRF.

Table 8-3 Configure the VRF attributes

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Enter the VRF instance configuration mode | **ip vrf** *vrf-name* | - |
| Enter the VRF IPv4 configuration mode | **address-family ipv4** | - |
| Enable the VRF MVPN function and enter the MVPN configuration mode | **mvpn** | Mandatory<br>By default, does not enable the MVPN function of the VRF instance. |
| Configure the MVPN RT of VRF | **route-target**<br>[ **both** \| **export** \| **import** ]<br>{ *ASN:nn* \| *IP-address:nn* } | Optional<br>By default, do not configure the MVPN RT attribute of the VRF. |

**Note:**

- When the VRF instance is not configured with MVPN RT, use the configured VPN RT as MVPN RT.

### Configure the PMSI Tunnel

PMSI (Provider Multicast Service Interface) is the logical channel for the public network to carry the multicast data flow of the private network, and the public network tunnel is the concrete realization form of PMSI. For the specified multicast data traffic, private multicast data traffic is distributed to other PEs through PMSI on Sender PE. Receiver PE receives multicast data traffic belonging to the same MVPN according to PMSI. PMSI can be divided into I-PMSI (Inclusive PMSI) and S-PMSI (Selective-PMSI).

At present, support the I-PMSI mLDP P2MP tunnel and I-PMSI RSVP-TE P2MP tunnel, which are initiated by Sender PE to set up, and just needs to be configured on Sender PE.

Table 8-4 Configure the PMSI tunnel

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Enter the VRF instance configuration mode | **ip vrf** *vrf-name* | - |
| Enter the VRF IPv4 configuration mode | **address-family ipv4** | - |
| Enable the VRF MVPN function and enter the MVPN configuration mode | **mvpn** | Mandatory<br>By default, do not enable the MVPN function of the VRF instance. |
| Configure the PMSI tunnel | **i-pmsi** { **mldp p2mp** \| **rsvp-te p2mp template** *template-name* } | Mandatory<br>By default, do not configure the PMSI tunnel. |

### Configure S-PMSI Tunnel Switching

In the NG MVPN network, when multicast data traffic is transmitted to multicast users through the I-PMSI tunnel, all PEs belonging to the same MVPN will receive multicast data traffic whether they have downstream recipients or not. When some PE sites have receivers and some PE sites have no receivers, there will be redundant data traffic in the network, waste bandwidth and increase the processing burden of PE.

S-PMSI tunnel switching can solve the above problems. After the multicast data traffic is switched from the I-PMSI tunnel to the S-PMSI tunnel, only the PE that needs multicast data traffic can receive it. Finally, the S-PMSI tunnel has no redundant data traffic, which saves bandwidth resources and reduces the processing burden of the PE device.

Table 8-5 Configure S-PMSI tunnel switching

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Enter the VRF instance configuration mode | **ip vrf** *vrf-name* | - |
| Enter the VRF IPv4 configuration mode | **address-family ipv4** | - |
| Enable the VRF MVPN function and enter the MVPN configuration mode | **mvpn** | Mandatory<br>By default, do not enable the MVPN function of the VRF instance. |
| Configure the S-PMSI switching address pool range and the switching conditions | **s-pmsi group** *group-address mask-len* [**source** *ip-address mask-len*] [**threshold** *threshold-value*] {**mldp p2mp** \| **rsvp-te p2mp template** *template-name* } [**limit** *number*] | Mandatory<br>By default, do not configure the S-PMSI switching address pool range and the switching conditions. |
| Configure the delay time of switching I-PMSI to SPMSI | **s-pmsi i2s-delay** *interval* | Optional<br>By default, the delay time of switching I-PMSI to S-PMSI is 5s. |
| Configure the delay time of switching S-PMSI to I-PMSI | **s-pmsi s2i-delay** *interval* | Optional<br>By default, the delay time of switching S-PMSI to I-PMSI is 5s. |
| Configure the delay time of deleting the S-PMSI tunnel | **s-pmsi tunnel-delete-delay** *interval* | Optional<br>By default, the delay time of deleting the S-PMSI tunnel is 5s. |

**Note:**

- The tunnel types of I-PMSI and S-PMSI are not required to be the same, but it is recommended to use the same tunnel type.

- When switching from the I-PMSI tunnel to the S-PMSI tunnel, the flow corresponding to the source group must be greater than or equal to the set value within a certain time.
- A single VPN can be configured with up to 16 S-PMSI switching address pool ranges.
- The limit value limits the number of the I-PMSI tunnels switched to S-PMSI tunnels within the address pool. When the multicast data stream entries meeting the switching conditions are greater than the limit value, only the specified number of tunnels will be switched. If the limit value is increased at this time, the previously unselected tunnels will be switched; If the limit value is reduced, the switched tunnel will not be switched back.
- The actual delay time of switching I-PMSI to S-PMSI is the configured delay + flow sampling time (100 seconds).
- The actual delay time for switching from S-PMSI to I-PMSI is the configured delay + flow sampling time (100 seconds).
- After switching from S-PMSI to I-PMSI timed out, if the traffic is still less than the switching threshold from I-PMSI to S-PMSI, start the tunnel-delete-delay timer.

## 8.2.2. Configure BGP MVPN Address Family

### Configure BGP MVPN Address Family

In NG MVPN network, PE is divided into Sender PE and Receiver PE. Sender PE and Receiver PE use MP-IBGP (multi-protocol extended BGP) MVPN address family to transmit the auto discovery route of the MVPN member and private multicast route. Usually, because multicast data traffic is transmitted between multicast source and multicast receiver, Sender PE should establish BGP MVPN neighborhood relationship with all Receiver PEs.

Table 8-6 Configure BGP MVPN address family

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Enter the BGP configuration mode | **router bgp** *autonomous-system* | - |
| Configure a BGP neighbor | **neighbor** { *neighbor-address* \| *peer-group-name* } **remote-as** *as-number* | Mandatory<br>By default, do not create any BGP neighbor. |
| Enter the BGP MVPN configuration mode | **address-family ipv4 mvpn** | - |
| Activate the MVPN address family of the PE neighbor | **neighbor** { *neighbor-address* \| *peer-group-name* } **activate** | Mandatory<br>By default, the BGP neighbors can only receive and send the IPv4 unicast route. |

**Note:**

- For the other optional neighbor configurations in the BGP MVPN address family, refer to BGP MVNP chapter of the command manual.

## 8.2.3. Configure MVPN ORF

### Configuration Conditions

Before configuring the MVPN ORF function, first complete the following tasks:

- Enable the BGP protocol.
- Configure the neighbor of the BGP MVPN address family and establish the session successfully.

### Configure MVPN ORF

In the NG MVPN environment of BGP, RR (Route Reflector) sends all MVPN routes (including AD routes and C-multicast routes) to peer-to-peer PE or RR. After the peer-to-peer PE or RR receives MVPN routes, it filters out unwanted AD routes according to the local configured MVPN IMPORT RT, and filters out unwanted C-multicast route according to the local generated C-multicast IMPORT RT. In large-scale NG MVPN network, a large number of unnecessary MVPN route information is advertised and filtered in the network, resulting in a large waste of resources. Especially, the performance of some edge PE devices is low. When receiving a large number of MVPN routes (mainly C-multicast routes generated when adding to the multicast group), the performance cannot be satisfied, which affects the normal NG MVPN service.

The basic principle of the MVPN ORF function is: The BGP router participating in MVPN route distribution advertises its own IMPORT RT by using MP-BGP, uses the standard BGP-4 best route selection algorithm to get the route distribution map of IMPORT RT, and takes the IMPORT information as ORF to perform the egress filtering for the MVPN route. In this way, the restriction advertising is made at the source of the MVPN route for the unnecessary MVPN route. In the practical network planning, RR usually plays the role, and the RR router generally has high performance.

Table 8-7 Configure the MVPN ORF function

| Step | Command | Description |
|---|---|---|
| Enter the global configuration mode | **configure terminal** | - |
| Enter the BGP configuration mode | **router bgp** *autonomous-system* | - |
| Enter the VPN-Target address family | **address-family ipv4 vpn-target** | - |
| Activate the VPN-Target address family of the neighbor | **neighbor {** *neighbor-address* **|** *peer-group-name***} active** | Mandatory<br>By default, the BGP neighbors can only receive and send the IPv4 unicast route. |

| Step | Command | Description |
|---|---|---|
| Enable the route reflection function in the VPN-Target address family mode | **neighbor {** *neighbor-address* **|** *peer-group-name* **} route-reflector-client** | Optional<br>By default, do not enable the route refection function. |
| In the VPN-Target address family mode, enable the RT egress filter function of the MVPN route | **neighbor** { *neighbor-address* **|** *peer-group-name* } **constraint-rt-filter-for-mvpn enable** | Mandatory<br>By default, do not perform the egress RT filter for the MVPN route. |

**Caution:**

- Activating a neighbor in the VPN-Target address family will activate the egress filtering function of the VPNv4 and VPNv6 routes of the neighbor.

### 8.2.4. NG MVPN Monitoring and Maintaining

Table 8-8 NG MVPN monitoring and maintaining

| Command | Description |
|---|---|
| **clear ip bgp** { ***** \| *neighbor-address* \| *as-number* \| **peer-group** *peer-group-name* \| **external** } [**vrf** *vrf-name* \| **ipv4 unicast** \| **ipv4 multicast** \| **vpnv4 unicast \| mvpn**] | Reset the BGP neighbor |
| **clear ip bgp** { ***** \| *neighbor-address* \| *as-number* \| **peer-group** *peer-group-name* \| **external** } [ **ipv4 unicast** \| **ipv4 multicast** \| **vpnv4 unicast** \| **mvpn** \| **vrf** *vrf-name* ] { [ **soft** ] [ **in** \| **out** ] } | Soft-reset the BGP neighbor |
| **show ip bgp ipv4 vpn-target [** *vpn-rt* **]** | Display the route information in the VPN-Target address family |
| **show ip bgp ipv4 vpn-target rt-filter** [ **neighbor** *ip-address* ] | Display the RT filter list of the neighbor; when not specifying the neighbor, display the RT filter list of all neighbors |
| **show ip bgp mvpn** {**all** \| **vrf** *vrf-name* \| **rd** *rd*} {**all-type** \| **type** [**1** [*A-D*] \| **3** [*S-PMSI-A-D*] \| **4** [*LEAF-A-D*] \| **5** [*SA-A-D*] \| **6** [*c-multicast-route*] \| **7** [*c-multicast-route*]]} | Display the route information in the BGP MVPN address family |

| Command | Description |
|---|---|
| **show ip bgp mvpn** { **all** \| **vrf** *vrf-name* \| **rd** *route-distinguisher* } { **neighbors** *ip-address* } { **advertised-routes** \| **received-routes** \| **routes** } { **all-type** \| **type 1** \| **type 3** \| **type 4** \| **type 5** \| **type 6** \| **type 7**} | Display the route information of the specified neighbor in the BGP MVPN address family |
| **show ip bgp mvpn** {**all** \| **vrf** *vrf-name* \| **rd** *route-distinguisher* \| **neighbors** *ip-address* } {**all-type** \| **type 1** \| **type 3** \| **type 4** \| **type 5** \| **type 6** \| **type 7**} { **statistics** } | Display the route statistics information in the BGP MVPN address family |
| **show ip bgp mvpn summary** | Display the summary information of all routes of MVPN |
| **show ip mvpn [vrf** *vrf-name* **]** | Display the MVPN abstract information |
| **show ip mvpn s-pmsi** [**vrf** *vrf-name* [**group** *group-address* [**source** *ip-address*]]] | Display the S-PMSI information |
| **show ip mvpn s-pmsi configuration** [**vrf** *vrf-name*] | Display the S-PMSI configuration information |
| **show ip mvpn s-pmsi mrt** [ **vrf** *vrf-name* [ **group** *group-address* [**source** *ip-address*] ] ] | Display the mrt information of S-PMSI |
| **show ip pim interface** [ *interface-name* ] [ **detail** ] [ **vrf** *vrf-name* ] | Display the PIM-SM interface information |
| **show ip pim mroute** [ **active** \| **proxy** \| **ssm** [ **active** ] \| **group** *group-ip-address* [ **source** *source-ip-address* ] \| **source** *source-ip-address* ] [ **vrf** *vrf-name* ] | Display the PIM-SM multicast route table information |
| **show ip pim neighbor** [ **detail** ] [ **vrf** *vrf-name* ] | Display the PIM-SM neighbor information |
| **show ip pim nexthop** [ *ip-address* ] [ **vrf** *vrf-name* ] | Display the PIM-SM next-hop router information |
| **show ip pim statistics** [ **vrf** *vrf-name* ] | Display the PIM-SM protocol packet statistics information |

## 8.3. NG MVPN Typical Configuration Example

### 8.3.1. Configure NG MVPN with the Adding Mode of Private Multicast as (S, G) and Public Tunnel as mLDP P2MP

#### Network Requirements

- There are two MVPNs in the network: VPN1 and VPN2. The two VPNs cannot access each other.
- CE1 and CE3 belong to VPN1, and CE2 and CE4 belong to VPN2.
- CE and PE use OSPF to advertise the private unicast route.
- In the autonomous domain, adopt OSPF as IGP to realize the intercommunication between Pes. Configure MP-IBGP to exchange the unicast VPN route information between PEs.
- VPN1 and VPN2 use mLDP P2MP as the public tunnel.
- VPN1 and VPN2 use PIM-SM as the multicast routing protocol.
- CE3 and CE4 directly connect the interfaces of the multicast receiver and run IGMPv3.
- Source sends the multicast flow, and the Receiver receives the multicast flow.

#### Network Topology

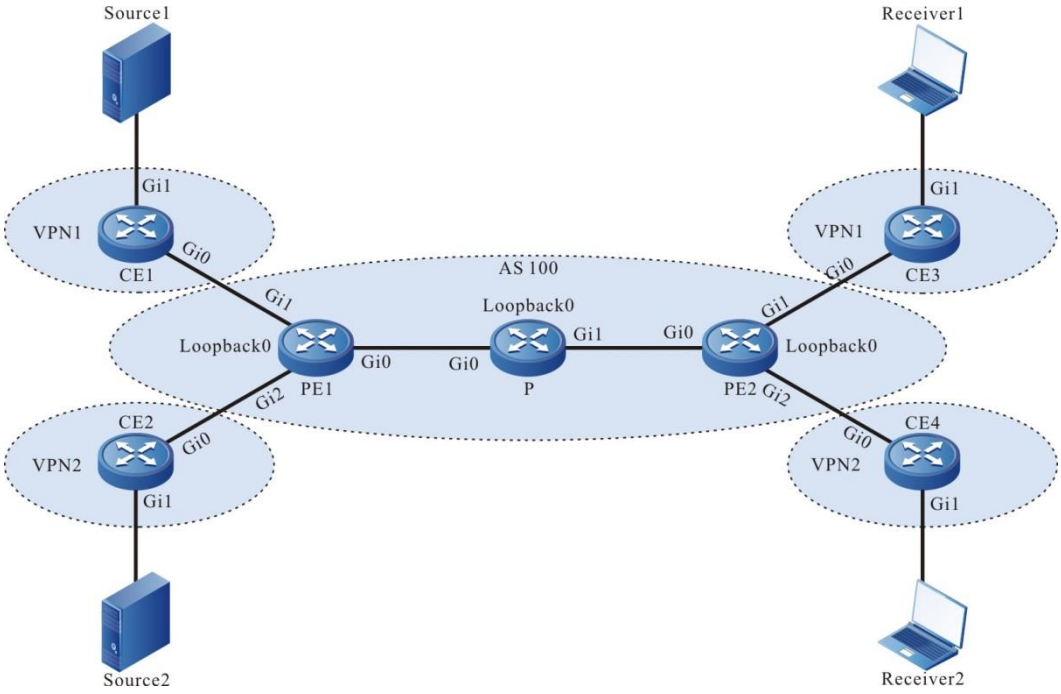


Figure 8-1 Configure NG MVPN with the adding mode of (S, G) and P-Tunnel type as mLDP P2MP in the domain

| Device | Interface | IP address | Device | Interface | IP address |
|---|---|---|---|---|---|
| CE1 | Gi0 | 14.1.1.2/16 | PE2 | Gi1 | 36.1.1.1/16 |
| | Gi1 | 40.1.1.1/16 | | Gi0/2/2 | 37.1.1.1/16 |
| PE1 | Gi0 | 12.1.1.1/16 | | Loopback0 | 3.3.3.3/32 |
| | Gi1 | 14.1.1.1/16 | CE3 | Gi0 | 36.1.1.2/16 |
| | Gi0/2/2 | 15.1.1.1/16 | | Gi1 | 60.1.1.1/16 |
| | Loopback0 | 1.1.1.1/32 | CE4 | Gi0 | 37.1.1.2/16 |
| CE2 | Gi0 | 15.1.1.2/16 | | Gi1 | 70.1.1.1/16 |
| | Gi1 | 50.1.1.1/32 | Source1 | | 40.1.1.2/16 |
| P | Gi0 | 12.1.1.2/16 | Source2 | | 50.1.1.2/16 |
| | Gi1 | 23.1.1.1/16 | Receiver1 | | 60.1.1.2/16 |
| | Loopback0 | 2.2.2.2/32 | Receiver2 | | 70.1.1.2/16 |
| PE2 | Gi0 | 23.1.1.2/16 | | | |

## Configuration Steps

**Step 1:** Configure the IP addresses of the interfaces. (omitted)

**Step 2:** Configure the global OSPF and advertise the global route.

#On PE1, configure the global OSPF.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
PE1(config-ospf)#network 12.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#On the P, configure the global OSPF.

```
P#configure terminal
P(config)#router ospf 100
```

```
P(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
P(config-ospf)#network 12.1.0.0 0.0.255.255 area 0
P(config-ospf)#network 23.1.0.0 0.0.255.255 area 0
P(config-ospf)#exit
```

#On PE2, configure the global OSPF.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
PE2(config-ospf)#network 23.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#After configuration, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route

Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management

    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   12.1.0.0/16 is directly connected, 00:23:28, gigabitethernet0
O   23.1.0.0/16 [110/2] via 12.1.1.2, 00:01:12, gigabitethernet0
C   1.1.1.1/32 is directly connected, 00:32:21, loopback0
O   2.2.2.2/32 [110/2] via 12.1.1.2, 00:01:12, gigabitethernet0
O   3.3.3.3/32 [110/3] via 12.1.1.2, 00:01:05, gigabitethernet0
```

You can see that there is the loopback port route information of P and PE2 in the global route table of PE1.

**Note:**

- For the checking method of P and PE2, refer to PE1.

**Step 3:** Enable MVPN, MPLS IP and MPLS LDP (containing MLDP P2MP).

#On PE1, enable the global MVPN, MPLS IP, and MPLS LDP (containing MLDP P2MP), and meanwhile, enable the MPLS IP and MPLS LDP on the interface.

```
PE1(config)#mvpn-id 1.1.1.1
PE1(config)#mpls ip
```

```
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#transport-address 1.1.1.1
PE1(config-ldp)#mldp p2mp
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#On P, enable the global MVPN, MPLS IP, and MPLS LDP (containing MLDP P2MP), and meanwhile, enable the MPLS IP and MPLS LDP on the interface.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 2.2.2.2
P(config-ldp)#transport-address 2.2.2.2
P(config-ldp)#mldp p2mp
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MVPN, MPLS IP, and MPLS LDP (containing MLDP P2MP), and meanwhile, enable the MPLS IP and MPLS LDP on the interface.

```
PE2(config)#mvpn-id 3.3.3.3
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 3.3.3.3
PE2(config-ldp)#transport-address 3.3.3.3
PE2(config-ldp)#mldp p2mp
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

**Note:**

- **router-id** and **transport-address** can be configured manually and also can be generated automatically. Usually, they are configured to be the same. If not configuring router-id and transport-address manually, the device will select automatically. From the up interfaces, first select the Loopback interface with the maximum IP address ; if the device is not configured with the Loopback interface address, select the common interface with the maximum IP address.

#After configuration, view the MVPN information on the device.

Take PE1 as an example:

```
PE1#show ip mvpn

 mvpn-id: 1.1.1.1
```

You can see that the MVPN ID of PE1 is 1.1.1.1.

#On the device, view the LDP and MLDP session information.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address    Peer Type     My Role   State        DeadTime
2.2.2.2            Multicast     Active    OPERATIONAL  00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0

PE1#show mpls ldp p2mp session
Session[2.2.2.2]:
   P2MP Capability: enable
   MBB Capability: disable
   Nexthop selected: 12.1.1.2
   Nexthop interface selected: gigabitethernet0
```

You can see that PE1 and P successfully set up the LDP session, and the session has the P2MP capability.

**Note:**

- For the checking method of P and PE2, refer to PE1.

**Step 4:** Configure the VPN instance, enable the MVPN and multicast forwarding of VRF, and advertise the CE route to PE via OSPF.

#On PE1, configure the VPN instance, enable MVPN and multicast forwarding, and configure the PIM-SM and OSPF in VPN1 and VPN2.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
```

```
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#address-family ipv4
PE1(config-vrf-ipv4)#mvpn
PE1(config-vrf-ipv4-mvpn)#i-pmsi mldp p2mp
PE1(config-vrf-ipv4-mvpn)#exit
PE1(config-vrf-ipv4)#exit
PE1(config-vrf)#exit
PE1(config)#ip vrf 2
PE1(config-vrf)#rd 200:1
PE1(config-vrf)#route-target export 200:1
PE1(config-vrf)#route-target import 200:1
PE1(config-vrf)#address-family ipv4
PE1(config-vrf-ipv4)#mvpn
PE1(config-vrf-ipv4-mvpn)#i-pmsi mldp p2mp
PE1(config-vrf-ipv4-mvpn)#exit
PE1(config-vrf-ipv4)#exit
PE1(config-vrf)#exit
PE1(config)#ip multicast-routing vrf 1
PE1(config)#ip multicast-routing vrf 2
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#ip vrf forwarding 1
PE1(config-if-gigabitethernet1)#ip address 14.1.1.1 255.255.0.0
PE1(config-if-gigabitethernet1)#ip pim sparse-mode
PE1(config-if-gigabitethernet1)#exit
PE1(config)#interface gigabitethernet0/2/2
PE1(config-if-gigabitethernet0/2/2)#ip vrf forwarding 2
PE1(config-if-gigabitethernet0/2/2)#ip address 15.1.1.1 255.255.0.0
PE1(config-if-gigabitethernet0/2/2)#ip pim sparse-mode
PE1(config-if-gigabitethernet0/2/2)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 14.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
PE1(config)#router ospf 300 vrf 2
PE1(config-ospf)#network 15.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#On CE1, enable the multicast forwarding, and configure PIM-SM and OSPF.

```
CE1(config)#ip multicast-routing
```

```
CE1(config)#interface gigabitethernet0
CE1(config-if-gigabitethernet0)#ip pim sparse-mode
CE1(config-if-gigabitethernet0)#exit
CE1(config)#interface gigabitethernet1
CE1(config-if-gigabitethernet1)#ip pim sparse-mode
CE1(config-if-gigabitethernet1)#exit
CE1(config)#router ospf 100
CE1(config-ospf)#network 14.1.0.0 0.0.255.255 area 0
CE1(config-ospf)#network 40.1.0.0 0.0.255.255 area 0
CE1(config-ospf)#exit
```

#On CE2, enable the multicast forwarding, and configure PIM-SM and OSPF.

```
CE2(config)#ip multicast-routing
CE2(config)#interface gigabitethernet0
CE2(config-if-gigabitethernet0)#ip pim sparse-mode
CE2(config-if-gigabitethernet0)#exit
CE2(config)#interface gigabitethernet1
CE2(config-if-gigabitethernet1)#ip pim sparse-mode
CE2(config-if-gigabitethernet1)#exit
CE2(config)#router ospf 100
CE2(config-ospf)#network 15.1.0.0 0.0.255.255 area 0
CE2(config-ospf)#network 50.1.0.0 0.0.255.255 area 0
CE2(config-ospf)#exit
```

#On PE2, configure the VPN instance, enable MVPN and multicast forwarding, and configure the PIM-SM and OSPF in VPN1 and VPN2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#address-family ipv4
PE2(config-vrf-ipv4)#mvpn
PE2(config-vrf-ipv4-mvpn)#i-pmsi mldp p2mp
PE2(config-vrf-ipv4-mvpn)#exit
PE2(config-vrf-ipv4)#exit
PE2(config-vrf)#exit
PE2(config)#ip vrf 2
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target export 200:1
```

```
PE2(config-vrf)#route-target import 200:1
PE2(config-vrf)#address-family ipv4
PE2(config-vrf-ipv4)#mvpn
PE2(config-vrf-ipv4-mvpn)#i-pmsi mldp p2mp
PE2(config-vrf-ipv4-mvpn)#exit
PE2(config-vrf-ipv4)#exit
PE2(config-vrf)#exit
PE2(config)#ip multicast-routing vrf 1
PE2(config)#ip multicast-routing vrf 2
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 36.1.1.1 255.255.0.0
PE2(config-if-gigabitethernet1)#ip pim sparse-mode
PE2(config-if-gigabitethernet1)#exit
PE2(config)#interface gigabitethernet0/2/2
PE2(config-if-gigabitethernet0/2/2)#ip vrf forwarding 2
PE2(config-if-gigabitethernet0/2/2)#ip address 37.1.1.1 255.255.0.0
PE2(config-if-gigabitethernet0/2/2)#ip pim sparse-mode
PE2(config-if-gigabitethernet0/2/2)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 36.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
PE2(config)#router ospf 300 vrf 2
PE2(config-ospf)#network 37.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#On CE3, enable multicast forwarding, configure PIM-SM and OSPF, and configure IGMPv3 on the interface connecting the multicast receiver.

```
CE3(config)#ip multicast-routing
CE3(config)#interface gigabitethernet0
CE3(config-if-gigabitethernet0)#ip pim sparse-mode
CE3(config-if-gigabitethernet0)#exit
CE3(config)#interface gigabitethernet1
CE3(config-if-gigabitethernet1)#ip pim sparse-mode
CE3(config-if-gigabitethernet1)#ip igmp version 3
CE3(config-if-gigabitethernet1)#exit
CE3(config)#router ospf 100
CE3(config-ospf)#network 36.1.0.0 0.0.255.255 area 0
```

```
CE3(config-ospf)#network 60.1.0.0 0.0.255.255 area 0
CE3(config-ospf)#exit
```

#On CE4, enable multicast forwarding, configure PIM-SM and OSPF, and configure IGMPv3 on the interface connecting the multicast receiver.

```
CE4(config)#ip multicast-routing
CE4(config)#interface gigabitethernet0
CE4(config-if-gigabitethernet0)#ip pim sparse-mode
CE4(config-if-gigabitethernet0)#exit
CE4(config)#interface gigabitethernet1
CE4(config-if-gigabitethernet1)#ip pim sparse-mode
CE4(config-if-gigabitethernet1)#ip igmp version 3
CE4(config-if-gigabitethernet1)#exit
CE4(config)#router ospf 100
CE4(config-ospf)#network 37.1.0.0 0.0.255.255 area 0
CE4(config-ospf)#network 70.1.0.0 0.0.255.255 area 0
CE4(config-ospf)#exit
```

#On PE, view the VPN route table and PIM-SM interface information.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   14.1.0.0/16 is directly connected, 00:11:45, gigabitethernet1
O   40.1.0.0/16 [110/2] via 14.1.1.2, 00:11:11, gigabitethernet1

PE1#show ip route vrf 2
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   15.1.0.0/16 is directly connected, 00:23:25, gigabitethernet0/2/2
O   50.1.0.0/16 [110/2] via 15.1.1.2, 00:22:53, gigabitethernet0/2/2
```

```
PE1#show ip pim interface vrf 1
PIM Interface Table:
PIM VRF Name: 1
Total 2 Interface entries
Total 1 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address         Interface                VIF    Ver/  VIF   Nbr   DR    DR          BSR
CISCO   Neighbor
                                         Index  Mode  Flag  Count Pri               Border
Neighbor Filter
14.1.1.1        gigabitethernet1         0      v2/S  UP    1     1     14.1.1.2      FALSE  FALSE
0.0.0.0         tunnel1023               2      v2/S  UP    0     1     0.0.0.0       FALSE
FALSE

PE1#show ip pim interface vrf 2
PIM Interface Table:
PIM VRF Name: 2
Total 2 Interface entries
Total 1 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address         Interface                VIF    Ver/  VIF   Nbr   DR    DR          BSR
CISCO   Neighbor
                                         Index  Mode  Flag  Count Pri               Border
Neighbor Filter
15.1.1.1        gigabitethernet0/2/2     0      v2/S  UP    1     1     15.1.1.2      FALSE
FALSE
0.0.0.0         tunnel1022               2      v2/S  UP    0     1     0.0.0.0       FALSE
FALSE
```

You can see that there are the routes to CE1 and CE2 in the VPN1 and VPN2 route tables of PE1, and the PIM-SM interface table contains the enabled PIM-SM interface and auto generated MVPN tunnel interface.

**Note:**

- For the checking methods of PE2, CE3, and CE4, refer to PE1.
- The PE at the multicast source should configure the tunnel type, and the PE at the multicast receiver does not need to configure the tunnel type.
- tunnel 1023 and tunnel1022 are the MVPN interface. When MVPN is enabled globally and on the VRF, each VPN will automatically generate one tunnel interface.

**Step 5:** Configure MP-IBGP, and use the loopback interface as the peer address; perform the route re-distribution with the IGP protocol in the VPN instance.

#On PE1, configure MP-IBGP, enable VPNv4, IPv4 MVPN address family; perform the route re-distribution with the IGP protocol in the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 3.3.3.3 remote-as 100
PE1(config-bgp)#neighbor 3.3.3.3 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 3.3.3.3 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 mvpn
PE1(config-bgp-af)#neighbor 3.3.3.3 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 2
PE1(config-bgp-af)#redistribute ospf 300
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
PE1(config)#router ospf 300 vrf 2
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#On PE2, configure MP-IBGP, enable VPNv4, IPv4 MVPN address family; perform the route re-distribution with the IGP protocol in the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 1.1.1.1 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 mvpn
PE2(config-bgp-af)#neighbor 1.1.1.1 activate
PE2(config-bgp-af)#exit-address-family
```

```
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 2
PE2(config-bgp-af)#redistribute ospf 300
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
PE2(config)#router ospf 300 vrf 2
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

**Note:**

- In practical applications, if there are two or more PE devices on the same site side, it is recommended that route should not be redistributed directly between different routing protocols. If you have to configure, you need to configure the routing policy to prevent generating the route loops.

**Step 6:** Check the result.

#After configuration, view the BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
3.3.3.3         4   100      40      41        6    0    0 00:32:01        4

Total number of neighbors 1
PE1#show ip bgp mvpn summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
3.3.3.3         4   100     527     539        6    0    0 00:03:32        2

Total number of neighbors 1
```

According to the numbers displayed in the State/PfxRcd column (the number of the route prefixes received from the neighbor), you can see that PE1 and PE2 successfully set up the BGP neighbor.

#On the PE, view the BGP VPNv4 route table, BGP MVPN route table, and the VPN route table.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 6, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[0]*> 14.1.0.0/16    0.0.0.0                  1         32768 ?
[0]*> 40.1.0.0/16    14.1.1.2                 2         32768 ?
[B]*>i36.1.0.0/16    3.3.3.3                  1    100      0 ?
[B]*>i60.1.0.0/16    3.3.3.3                  2    100      0 ?

PE1#show ip bgp vpnv4 vrf 2
BGP table version is 6, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 200:1 (Default for VRF 2)
[0]*> 15.1.0.0/16    0.0.0.0                  1         32768 ?
[0]*> 50.1.0.0/16    15.1.1.2                 2         32768 ?
[B]*>i37.1.0.0/16    3.3.3.3                  1    100      0 ?
[B]*>i70.1.0.0/16    3.3.3.3                  2    100      0 ?

PE1#show ip bgp mvpn vrf 1 all-type
BGP local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

MVPN Information for Route Distinguisher:100:1 (Default for VRF 1)

Intra-AS I-PMSI A-D Routes:

| Network(Originating IP Addr) | Next Hop | Metric | LocPrf | Weight | Path |
|---|---|---|---|---|---|
| [B]*> 1.1.1.1 | 0.0.0.0 | 0 | | 32768 | i |
| [B]*>i3.3.3.3 | 3.3.3.3 | 0 | 100 | 0 | i |

PE1#show ip bgp mvpn vrf 2 all-type

BGP local router ID is 1.1.1.1

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

MVPN Information for Route Distinguisher:200:1 (Default for VRF 2)

Intra-AS I-PMSI A-D Routes:

| Network(Originating IP Addr) | Next Hop | Metric | LocPrf | Weight | Path |
|---|---|---|---|---|---|
| [B]*> 1.1.1.1 | 0.0.0.0 | 0 | | 32768 | i |
| [B]*>i3.3.3.3 | 3.3.3.3 | 0 | 100 | 0 | i |

PE1#show ip route vrf 1

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management

D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 36.1.0.0/16 [200/1] via 3.3.3.3, 00:01:06, gigabitethernet0

C 14.1.0.0/16 is directly connected, 00:23:25, gigabitethernet1

O 40.1.0.0/16 [110/2] via 14.1.1.2, 00:22:51, gigabitethernet1

B 60.1.0.0/16 [200/2] via 3.3.3.3, 00:01:06, gigabitethernet0

PE1#show ip route vrf 2

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management

D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 37.1.0.0/16 [200/1] via 3.3.3.3, 00:01:15, gigabitethernet0

C 15.1.0.0/16 is directly connected, 00:23:25, gigabitethernet0/2/2

```
O   50.1.0.0/16 [110/2] via 15.1.1.2, 00:22:53, gigabitethernet0/2/2
B   70.1.0.0/16 [200/2] via 3.3.3.3, 00:01:15, gigabitethernet0
```

You can see that there are the routes to the peer CE3 and CE4 in the BGP VPNv4 route table, VPN1 and VPN2 route tables of PE1. There is type-1 MVPN route information advertised by the peer PE2 in the BGP MVPN route table of PE1.

#On the PE, view the PIM-SM neighbor information.

Take PE1 as an example:

```
PE1#show ip pim neighbor vrf 1
PIM Neighbor Table:
PIM VRF Name: 1
Total 2 Neighbor entry

Neighbor        Interface              Uptime/Expires     Ver   DR
Address                                                        Priority/Mode
3.3.3.3         tunnel1023             00:19:51/never     v2    N / DR
14.1.1.2        gigabitethernet1       00:45:46/00:01:42  v2    1 / DR

PE1#show ip pim neighbor vrf 2
PIM Neighbor Table:
PIM VRF Name: 2
Total 2 Neighbor entry

Neighbor        Interface              Uptime/Expires     Ver   DR
Address                                                        Priority/Mode
3.3.3.3         tunnel1022             00:20:08/never     v2    N / DR
15.1.1.2        gigabitethernet0/2/2   00:37:21/00:01:37  v2    1 / DR
```

You can see that PE1 sets up the PIM-SM neighbor with CE1, CE2, and sets up the PIM-SM neighbor with the MVPN tunnel interface of the peer PE.

**Note:**

- For the checking method of PE2, refer to PE1.

#Receiver1 is added to IGMPv3 group 225.0.0.1, and is specified to receive the multicast flow sent by the multicast source Source1 and Source2.

Receiver2 is added to IGMPv3 group 226.0.0.1, and is specified to receive the multicast flow sent by the multicast source Source1 and Source2.

On CE3 and CE4, view the IGMP group and PIM-SM route table.

```
CE3#show ip igmp groups detail
Interface: gigabitethernet1
```

```
Group:        225.0.0.1
Uptime:       00:00:10
Group mode:    Include
Last reporter:  60.1.1.2
TIB-A Count:   2
TIB-B Count:   0
Group source list: (R - Remote, M - SSM Mapping)
  Source Address  Uptime    v3 Exp    M Exp    Fwd  Flags
  40.1.1.2        00:00:10  00:04:14  stopped  Yes  R
  50.1.1.2        00:00:10  00:04:14  stopped  Yes  R

CE4#show ip igmp groups detail
Interface: gigabitethernet1
Group:        226.0.0.1
Uptime:       00:00:10
Group mode:    Include
Last reporter:  70.1.1.2
TIB-A Count:   2
TIB-B Count:   0
Group source list: (R - Remote, M - SSM Mapping)
  Source Address  Uptime    v3 Exp    M Exp    Fwd  Flags
  40.1.1.2        00:00:10  00:04:14  stopped  Yes  R
  50.1.1.2        00:00:10  00:04:14  stopped  Yes  R

CE3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 2 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(40.1.1.2, 225.0.0.1)
Up time: 00:03:20
```

```
KAT time: 00:00:10
RPF nbr: 36.1.1.1
RPF idx: gigabitethernet0
SPT bit: FALSE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    gigabitethernet1
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 0

(50.1.1.2, 225.0.0.1)
Up time: 00:03:20
KAT time: 00:00:10
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: FALSE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    gigabitethernet1
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 0

CE4#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
```

```
Total 2 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(40.1.1.2, 226.0.0.1)
Up time: 00:03:20
KAT time: 00:00:10
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: FALSE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    gigabitethernet1
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 0

(50.1.1.2, 226.0.0.1)
Up time: 00:03:20
KAT time: 00:00:10
RPF nbr: 37.1.1.1
RPF idx: gigabitethernet0
SPT bit: FALSE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    gigabitethernet1
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
```

```
    gigabitethernet1
  Packet count 0
```

You can see that the group is added on CE3 and CE4 successfully, and the (S,G) route is generated. CE3 and CE2 are not in one VPN, and there is no unicast route to Source2, so only send the (S,G) route to Source1. CE4 is similar.

#On the PE, view the BGP MVPN type-7 route table.

```
PE1#show ip bgp mvpn rd 100:1 type 7
BGP local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
MVPN Information for Route Distinguisher:100:1 (Default for VRF 1)
 Source Tree Join Routes:
    Network(AS Number:C-S:C-G)     Next Hop          Metric    LocPrf Weight Path
[B]*>i100:40.1.1.2:225.0.0.1        3.3.3.3              0       100     0 i

PE1#show ip bgp mvpn rd 200:1 type 7
BGP local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
MVPN Information for Route Distinguisher:200:1 (Default for VRF 2)
 Source Tree Join Routes:
    Network(AS Number:C-S:C-G)     Next Hop          Metric    LocPrf Weight Path
[B]*>i100:50.1.1.2:226.0.0.1        3.3.3.3              0       100     0 i

PE2#show ip bgp mvpn rd 100:1 type 7
BGP local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
MVPN Information for Route Distinguisher:100:1
 Source Tree Join Routes:
    Network(AS Number:C-S:C-G)     Next Hop          Metric    LocPrf Weight Path
[B]*> 100:40.1.1.2:225.0.0.1        0.0.0.0              0          32768 i

PE2#show ip bgp mvpn rd 200:1 type 7
BGP local router ID is 3.3.3.3
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
MVPN Information for Route Distinguisher:200:1
 Source Tree Join Routes:
    Network(AS Number:C-S:C-G)     Next Hop          Metric     LocPrf Weight Path
[B]*> 100:50.1.1.2:226.0.0.1       0.0.0.0           0          32768 i
```

#On the PE, view the PIM-SM route table of the VPN.

```
PE1#show ip pim mroute vrf 1
IP Multicast Routing Table:
PIM VRF Name: 1
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(40.1.1.2, 225.0.0.1)
Up time: 00:02:50
KAT time: 00:00:40
RPF nbr: 14.1.1.2
RPF idx: gigabitethernet1
SPT bit: FALSE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    tunnel1023  00:02:50/stopped
  Asserted interface list:
  Outgoing interface list:
    tunnel1023
  Packet count 0

PE1#show ip pim mroute vrf 2
```

```
IP Multicast Routing Table:
PIM VRF Name: 2
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(50.1.1.2, 226.0.0.1)
Up time: 00:02:55
KAT time: 00:00:35
RPF nbr: 15.1.1.2
RPF idx: gigabitethernet0/2/2
SPT bit: FALSE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    tunnel1022  00:02:55/stopped
  Asserted interface list:
  Outgoing interface list:
    tunnel1022
  Packet count 0

PE2#show ip pim mroute vrf 1
IP Multicast Routing Table:
PIM VRF Name: 1
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer
```

```
(40.1.1.2, 225.0.0.1)
Up time: 00:03:20
KAT time: 00:00:10
RPF nbr: 1.1.1.1
RPF idx: tunnel1023
SPT bit: FALSE
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
 Joined interface list:
  gigabitethernet1  00:03:20/00:02:10
 Asserted interface list:
 Outgoing interface list:
  gigabitethernet1
 Packet count 0

PE2#show ip pim mroute vrf 2
IP Multicast Routing Table:
PIM VRF Name: 2
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(50.1.1.2, 226.0.0.1)
Up time: 00:03:20
KAT time: 00:00:10
RPF nbr: 1.1.1.1
RPF idx: tunnel1022
SPT bit: FALSE
Flags:
 JOIN DESIRED
```

```
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    gigabitethernet0/2/2  00:03:20/00:02:10
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet0/2/2
  Packet count 0
```

You can see that both PE1 and PE2 have the corresponding multicast route, and the egress interface information is correct. Source1 and Source2 send the corresponding multicast flow. Receiver1 can only receive the multicast flow sent by Source1, and Receiver2 can only receive the multicast flow sent by Source2.

**Note:**

- For the checking method of CE1 and CE2, refer to PE1.

### 8.3.2. Configure NG MVPN with the Adding Mode of Private Multicast as (S, G) and Public Tunnel as RSVP-TE P2MP

#### Network Requirements

- There are two MVPNs in the network: VPN1 and VPN2. The two VPNs cannot access each other.
- CE1 and CE3 belong to VPN1, and CE2 and CE4 belong to VPN2.
- CE and PE use OSPF to advertise the private unicast route.
- In the autonomous domain, adopt OSPF as IGP to realize the intercommunication between PEs. Configure MP-IBGP to exchange the unicast VPN route information between PEs.
- VPN1 and VPN2 use RSVP-TE P2MP as the public tunnel.
- VPN1 and VPN2 use PIM-SM as the multicast routing protocol.
- CE3 and CE4 directly connect the interfaces of the multicast receiver and run IGMPv3.
- Source sends the multicast flow, and the Receiver receives the multicast flow.

## Network Topology

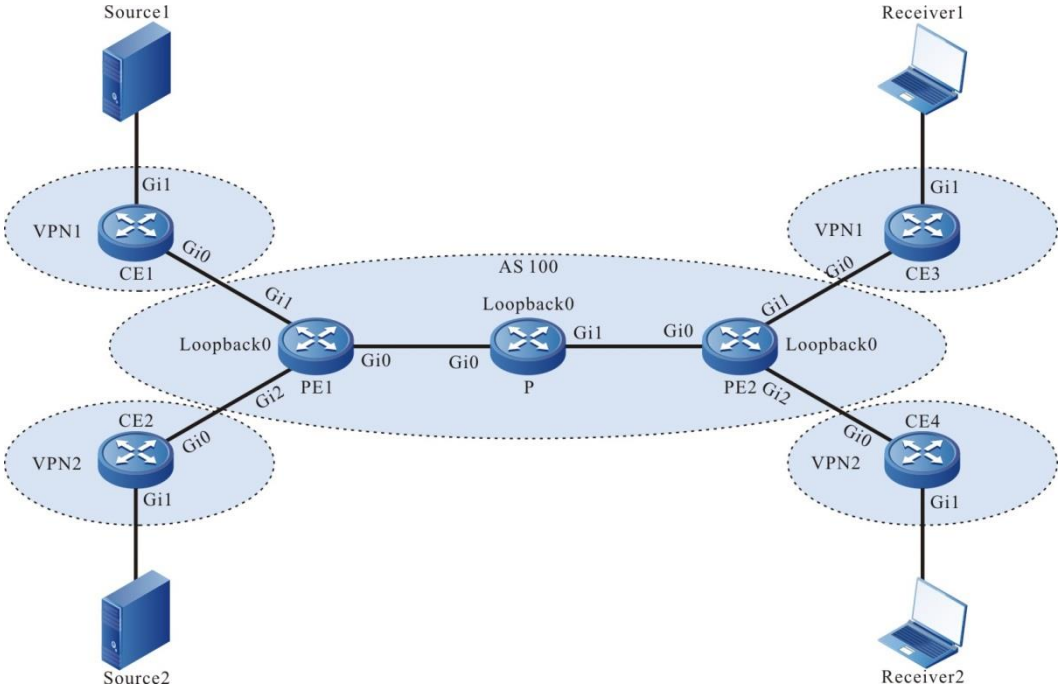


Figure 8-2 Configure NG MVPN with the adding mode of (S, G) and P-Tunnel type as RSVP-TE P2MP in the domain

| Device | Interface | IP address | Device | Interface | IP address |
|---|---|---|---|---|---|
| CE1 | Gi0 | 14.1.1.2/16 | PE2 | Gi1 | 36.1.1.1/16 |
| | Gi1 | 40.1.1.1/16 | | Gi0/2/2 | 37.1.1.1/16 |
| PE1 | Gi0 | 12.1.1.1/16 | | Loopback0 | 3.3.3.3/32 |
| | Gi1 | 14.1.1.1/16 | CE3 | Gi0 | 36.1.1.2/16 |
| | Gi0/2/2 | 15.1.1.1/16 | | Gi1 | 60.1.1.1/16 |
| | Loopback0 | 1.1.1.1/32 | CE4 | Gi0 | 37.1.1.2/16 |
| CE2 | Gi0 | 15.1.1.2/16 | | Gi1 | 70.1.1.1/16 |
| | Gi1 | 50.1.1.1/32 | Source1 | | 40.1.1.2/16 |

| Device | Interface | IP address | Device | Interface | IP address |
|---|---|---|---|---|---|
| P | Gi0 | 12.1.1.2/16 | Source2 | | 50.1.1.2/16 |
| | Gi1 | 23.1.1.1/16 | Receiver1 | | 60.1.1.2/16 |
| | Loopback0 | 2.2.2.2/32 | Receiver2 | | 70.1.1.2/16 |
| PE2 | Gi0 | 23.1.1.2/16 | | | |

## Configuration Steps

**Step 1:** Configure the IP addresses of the interfaces. (omitted)

**Step 2:** Configure the OSPF protocol, all interfaces cover to area 0, and enable the MPLS TE capability in area 0 of Device1, Device2, and Device3.

#On PE1, configure the global OSPF, and enable the MPLS TE capability in area 0.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#mpls traffic-eng area 0
PE1(config-ospf)#mpls traffic-eng router-id 1.1.1.1
PE1(config-ospf)#router-id 1.1.1.1
PE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
PE1(config-ospf)#network 12.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#On P, configure the global OSPF, and enable the MPLS TE capability in area 0.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#mpls traffic-eng area 0
P(config-ospf)#mpls traffic-eng router-id 2.2.2.2
P(config-ospf)#router-id 2.2.2.2
P(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
P(config-ospf)#network 12.1.0.0 0.0.255.255 area 0
P(config-ospf)#network 23.1.0.0 0.0.255.255 area 0
P(config-ospf)#exit
```

#On PE2, configure the global OSPF, and enable the MPLS TE capability in area 0.

```
PE2#configure terminal
PE2(config)#router ospf 100
```

```
PE2(config-ospf)#mpls traffic-eng area 0
PE2(config-ospf)#mpls traffic-eng router-id 3.3.3.3
PE2(config-ospf)#router-id 3.3.3.3
PE2(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
PE2(config-ospf)#network 23.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#After configuration, query the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route

Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management

    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

LC  1.1.1.1/32 is directly connected, 16:19:56, loopback0
O   2.2.2.2/32 [110/2] via 12.1.1.2, 00:06:14, gigabitethernet0
O   3.3.3.3/32 [110/3] via 12.1.1.2, 00:05:54, gigabitethernet0
C   12.1.0.0/16 is directly connected, 00:07:51, gigabitethernet0
L   12.1.1.1/32 is directly connected, 00:07:51, gigabitethernet0
O   23.1.0.0/16 [110/2] via 12.1.1.2, 00:06:14, gigabitethernet0
```

You can see that there is the loopback port route information of P and PE2 in the global route table of PE1.

**Note:**

- For the checking method of P and PE2, refer to PE1.

**Step 3:** Enable MVPN, MPLS IP, MPLS LDP, and MPLS TE.

#On PE1, enable the global MVPN, MPLS IP, MPLS LDP, and MPLS TE, and meanwhile, enable the MPLS IP, MPLS LDP, and MPLS TE on the interface. Configure the maximum reversible bandwidth of the link as 100000 kbps on interface gigabitethernet0.

```
PE1(config)#mvpn-id 1.1.1.1
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#transport-address 1.1.1.1
```

```
PE1(config-ldp)#exit
PE1(config)#mpls traffic-eng tunnels
PE1(config-rsvp-te)#p2mp
PE1(config-rsvp-te)#router-id 1.1.1.1
PE1(config-rsvp-te)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#mpls traffic-eng tunnels
PE1(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
PE1(config-if-gigabitethernet0)#exit
```

#On P, enable the global MVPN, MPLS IP, MPLS LDP, and MPLS TE, and meanwhile, enable the MPLS IP, MPLS LDP, and MPLS TE on the interface. Configure the maximum reversible bandwidth of the link as 100000 kbps on interface gigabitethernet0 and gigabitethernet1.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 2.2.2.2
P(config-ldp)#transport-address 2.2.2.2
P(config-ldp)#exit
P(config)#mpls traffic-eng tunnels
P(config-rsvp-te)#p2mp
P(config-rsvp-te)#router-id 2.2.2.2
P(config-rsvp-te)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#mpls traffic-eng tunnels
P(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#mpls traffic-eng tunnels
P(config-if-gigabitethernet1)#ip rsvp bandwidth 100000
P(config-if-gigabitethernet1)#exit
```

#On PE2, enable the global MVPN, MPLS IP, MPLS LDP, and MPLS TE, and meanwhile, enable the MPLS IP, MPLS LDP, and MPLS TE on the interface. Configure the maximum reversible bandwidth of the link as 100000 kbps on interface gigabitethernet0.

```
PE2(config)#mvpn-id 3.3.3.3
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 3.3.3.3
PE2(config-ldp)#transport-address 3.3.3.3
PE2(config-ldp)#exit
PE2(config)#mpls traffic-eng tunnels
PE2(config-rsvp-te)#p2mp
PE2(config-rsvp-te)#router-id 3.3.3.3
PE2(config-rsvp-te)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#mpls traffic-eng tunnels
PE2(config-if-gigabitethernet0)#ip rsvp bandwidth 100000
PE2(config-if-gigabitethernet0)#exit
```

**Note:**

- **router-id** and **transport-address** can be configured manually and also can be generated automatically. Usually, they are configured to be the same. If not configuring router-id and transport-address manually, the device will select automatically. From the up interfaces, first select the Loopback interface with the maximum IP address ; if the device is not configured with the Loopback interface address, select the common interface with the maximum IP address.

#After configuration, view the MVPN information on the device.

Take PE1 as an example:

```
PE1#show ip mvpn

 mvpn-id: 1.1.1.1
```

You can see that the MVPN ID of PE1 is 1.1.1.1.

#On the device, view the LDP session information.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address   Peer Type    My Role  State        DeadTime
2.2.2.2           Multicast    Active   OPERATIONAL  00:02:26
Statistics for ldp sessions:
    Multicast sessions: 1
    Targeted sessions: 0
```

You can see that PE1 and P successfully set up the LDP session

**Note:**

- For the checking method of P and PE2, refer to PE1.

**Step 4:** Configure the VPN instance, enable the MVPN and multicast forwarding of VRF, configure the MPLS TE P2MP profile, and advertise the CE route to PE via OSPF.

#On PE1, configure the VPN instance, enable MVPN and multicast forwarding, configure the MPLS TE P2MP profile, and configure the PIM-SM and OSPF in VPN1 and VPN2.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#address-family ipv4
PE1(config-vrf-ipv4)#mvpn
PE1(config-vrf-ipv4-mvpn)#i-pmsi rsvp-te p2mp template 1
PE1(config-vrf-ipv4-mvpn)#exit
PE1(config-vrf-ipv4)#exit
PE1(config-vrf)#exit
PE1(config)#ip vrf 2
PE1(config-vrf)#rd 200:1
PE1(config-vrf)#route-target export 200:1
PE1(config-vrf)#route-target import 200:1
PE1(config-vrf)#address-family ipv4
PE1(config-vrf-ipv4)#mvpn
PE1(config-vrf-ipv4-mvpn)#i-pmsi rsvp-te p2mp template 2
PE1(config-vrf-ipv4-mvpn)#exit
PE1(config-vrf-ipv4)#exit
PE1(config-vrf)#exit
PE1(config)#ip multicast-routing vrf 1
PE1(config)#ip multicast-routing vrf 2
PE1(config)#mpls traffic-eng p2mp-template 1
PE1(config-te-p2mp-template)#tunnel mpls traffic-eng bandwidth 1000
PE1(config-te-p2mp-template)#exit
PE1(config)#mpls traffic-eng p2mp-template 2
PE1(config-te-p2mp-template)#tunnel mpls traffic-eng bandwidth 1000
PE1(config-te-p2mp-template)#exit
PE1(config)#interface gigabitethernet1
```

```
PE1(config-if-gigabitethernet1)#ip vrf forwarding 1
PE1(config-if-gigabitethernet1)#ip address 14.1.1.1 255.255.0.0
PE1(config-if-gigabitethernet1)#ip pim sparse-mode
PE1(config-if-gigabitethernet1)#exit
PE1(config)#interface gigabitethernet0/2/2
PE1(config-if-gigabitethernet0/2/2)#ip vrf forwarding 2
PE1(config-if-gigabitethernet0/2/2)#ip address 15.1.1.1 255.255.0.0
PE1(config-if-gigabitethernet0/2/2)#ip pim sparse-mode
PE1(config-if-gigabitethernet0/2/2)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 14.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
PE1(config)#router ospf 300 vrf 2
PE1(config-ospf)#network 15.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#On CE1, enable multicast forwarding, and configure PIM-SM and OSPF.

```
CE1(config)#ip multicast-routing
CE1(config)#interface gigabitethernet0
CE1(config-if-gigabitethernet0)#ip pim sparse-mode
CE1(config-if-gigabitethernet0)#exit
CE1(config)#interface gigabitethernet1
CE1(config-if-gigabitethernet1)#ip pim sparse-mode
CE1(config-if-gigabitethernet1)#exit
CE1(config)#router ospf 100
CE1(config-ospf)#network 14.1.0.0 0.0.255.255 area 0
CE1(config-ospf)#network 40.1.0.0 0.0.255.255 area 0
CE1(config-ospf)#exit
```

#On CE2, enable multicast forwarding, and configure PIM-SM and OSPF.

```
CE2(config)#ip multicast-routing
CE2(config)#interface gigabitethernet0
CE2(config-if-gigabitethernet0)#ip pim sparse-mode
CE2(config-if-gigabitethernet0)#exit
CE2(config)#interface gigabitethernet1
CE2(config-if-gigabitethernet1)#ip pim sparse-mode
CE2(config-if-gigabitethernet1)#exit
CE2(config)#router ospf 100
CE2(config-ospf)#network 15.1.0.0 0.0.255.255 area 0
```

```
CE2(config-ospf)#network 50.1.0.0 0.0.255.255 area 0
CE2(config-ospf)#exit
```

#On PE2, configure the VPN instance, enable MVPN and multicast forwarding, and configure the PIM-SM and OSPF in VPN1 and VPN2.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#address-family ipv4
PE2(config-vrf-ipv4)#mvpn
PE2(config-vrf-ipv4-mvpn)#exit
PE2(config-vrf-ipv4)#exit
PE2(config-vrf)#exit
PE2(config)#ip vrf 2
PE2(config-vrf)#rd 200:1
PE2(config-vrf)#route-target export 200:1
PE2(config-vrf)#route-target import 200:1
PE2(config-vrf)#address-family ipv4
PE2(config-vrf-ipv4)#mvpn
PE2(config-vrf-ipv4-mvpn)#exit
PE2(config-vrf-ipv4)#exit
PE2(config-vrf)#exit
PE2(config)#ip multicast-routing vrf 1
PE2(config)#ip multicast-routing vrf 2
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 36.1.1.1 255.255.0.0
PE2(config-if-gigabitethernet1)#ip pim sparse-mode
PE2(config-if-gigabitethernet1)#exit
PE2(config)#interface gigabitethernet0/2/2
PE2(config-if-gigabitethernet0/2/2)#ip vrf forwarding 2
PE2(config-if-gigabitethernet0/2/2)#ip address 37.1.1.1 255.255.0.0
PE2(config-if-gigabitethernet0/2/2)#ip pim sparse-mode
PE2(config-if-gigabitethernet0/2/2)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 36.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

```
PE2(config)#router ospf 300 vrf 2
PE2(config-ospf)#network 37.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#On CE3, enable multicast forwarding, configure the PIM-SM and OSPF, and configure IGMPv3 on the interface of connecting the multicast receiver.

```
CE3(config)#ip multicast-routing
CE3(config)#interface gigabitethernet0
CE3(config-if-gigabitethernet0)#ip pim sparse-mode
CE3(config-if-gigabitethernet0)#exit
CE3(config)#interface gigabitethernet1
CE3(config-if-gigabitethernet1)#ip pim sparse-mode
CE3(config-if-gigabitethernet1)#ip igmp version 3
CE3(config-if-gigabitethernet1)#exit
CE3(config)#router ospf 100
CE3(config-ospf)#network 36.1.0.0 0.0.255.255 area 0
CE3(config-ospf)#network 60.1.0.0 0.0.255.255 area 0
CE3(config-ospf)#exit
```

#On CE4, enable multicast forwarding, configure the PIM-SM and OSPF, and configure IGMPv3 on the interface of connecting the multicast receiver.

```
CE4(config)#ip multicast-routing
CE4(config)#interface gigabitethernet0
CE4(config-if-gigabitethernet0)#ip pim sparse-mode
CE4(config-if-gigabitethernet0)#exit
CE4(config)#interface gigabitethernet1
CE4(config-if-gigabitethernet1)#ip pim sparse-mode
CE4(config-if-gigabitethernet1)#ip igmp version 3
CE4(config-if-gigabitethernet1)#exit
CE4(config)#router ospf 100
CE4(config-ospf)#network 37.1.0.0 0.0.255.255 area 0
CE4(config-ospf)#network 70.1.0.0 0.0.255.255 area 0
CE4(config-ospf)#exit
```

**Step 5:** Configure MP-IBGP, and use the loopback interface as the peer address; perform the route re-distribution with the IGP protocol in the VPN instance.

#On PE1, configure MP-IBGP, enable VPNv4, IPv4 MVPN address family; perform the route re-distribution with the IGP protocol in the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 3.3.3.3 remote-as 100
PE1(config-bgp)#neighbor 3.3.3.3 update-source loopback0
```

```
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 3.3.3.3 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 mvpn
PE1(config-bgp-af)#neighbor 3.3.3.3 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 2
PE1(config-bgp-af)#redistribute ospf 300
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
PE1(config)#router ospf 300 vrf 2
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#On PE2, configure MP-IBGP, enable VPNv4, IPv4 MVPN address family; perform the route re-distribution with the IGP protocol in the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 1.1.1.1 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 mvpn
PE2(config-bgp-af)#neighbor 1.1.1.1 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 2
PE2(config-bgp-af)#redistribute ospf 300
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
```

```
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
PE2(config)#router ospf 300 vrf 2
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

**Note:**

- In practical applications, if there are two or more PE devices on the same site side, it is recommended that route should not be redistributed directly between different routing protocols. If you have to configure, you need to configure the routing policy to prevent generating the route loops.

**Step 5:** Check the result.

#After configuration, query the BGP neighbor information on PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
1 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
3.3.3.3         4   100      18      11        2    0    0 00:01:30        4

Total number of neighbors 1

PE1#show ip bgp mvpn summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 4
1 BGP AS-PATH entries
1 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
3.3.3.3         4   100      18      11        4    0    0 00:01:30        4

Total number of neighbors 1
```

According to the numbers displayed in the State/PfxRcd column (the number of the route prefixes received from the neighbor), you can see that PE1 and PE2 successfully set up the BGP neighbor.

#On the PE, view the BGP VPNv4 route table, BGP MVPN route table, and the VPN route table. Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 6, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[0]*> 14.1.0.0/16       0.0.0.0                1         32768 ?
[0]*> 40.1.0.0/16       14.1.1.2               2         32768 ?
[B]*>i36.1.0.0/16       3.3.3.3                  1    100      0 ?
[B]*>i60.1.0.0/16       3.3.3.3                  2    100      0 ?

PE1#show ip bgp vpnv4 vrf 2
BGP table version is 6, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 200:1 (Default for VRF 2)
[0]*> 15.1.0.0/16       0.0.0.0                1         32768 ?
[0]*> 50.1.0.0/16       15.1.1.2               2         32768 ?
[B]*>i37.1.0.0/16       3.3.3.3                  1    100      0 ?
[B]*>i70.1.0.0/16       3.3.3.3                  2    100      0 ?

PE1#show ip bgp mvpn vrf 1 all-type
BGP local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
MVPN Information for Route Distinguisher:100:1 (Default for VRF 1)
 Intra-AS I-PMSI A-D Routes:
     Network(Originating IP Addr)    Next Hop          Metric     LocPrf Weight Path
[B]*> 1.1.1.1                    0.0.0.0                0          32768 i
[B]*>i3.3.3.3                      3.3.3.3                0       100      0 i
```

```
PE1#show ip bgp mvpn vrf 2 all-type
BGP local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
MVPN Information for Route Distinguisher:200:1 (Default for VRF 2)
 Intra-AS I-PMSI A-D Routes:
     Network(Originating IP Addr)   Next Hop          Metric     LocPrf Weight Path
[B]*> 1.1.1.1                      0.0.0.0             0          32768 i
[B]*>i3.3.3.3                        3.3.3.3             0       100      0 i

PE1#show ip route vrf 1
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M -
Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   36.1.0.0/16 [200/1] via 3.3.3.3, 00:01:06, gigabitethernet0
C   14.1.0.0/16 is directly connected, 00:23:25, gigabitethernet1
L   14.1.1.1/32 is directly connected, 00:23:25, gigabitethernet1
O   40.1.0.0/16 [110/2] via 14.1.1.2, 00:22:51, gigabitethernet1
B   60.1.0.0/16 [200/2] via 3.3.3.3, 00:01:06, gigabitethernet0

PE1#show ip route vrf 2
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M -
Management
      D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   37.1.0.0/16 [200/1] via 3.3.3.3, 00:01:15, gigabitethernet0
C   15.1.0.0/16 is directly connected, 00:23:25, gigabitethernet0/2/2
L   15.1.1.1/32 is directly connected, 00:23:25, gigabitethernet0/2/2
O   50.1.0.0/16 [110/2] via 15.1.1.2, 00:22:53, gigabitethernet0/2/2
B   70.1.0.0/16 [200/2] via 3.3.3.3, 00:01:15, gigabitethernet0
```

You can see that there are the routes to the peer CE3 and CE4 in the BGP VPNv4 route table, VPN1 and VPN2 route tables of PE1. There is type-1 MVPN route information advertised by the peer PE2 in the BGP MVPN route table of PE1.

#On the PE, query the PIM-SM neighbor information.

Take PE1 as an example:

```
PE1#show ip pim neighbor vrf 1
PIM Neighbor Table:
PIM VRF Name: 1
Total 2 Neighbor entry

Neighbor        Interface              Uptime/Expires     Ver   DR
Address                                                        Priority/Mode
3.3.3.3         tunnel1023             00:19:51/never     v2    N / DR
14.1.1.2        gigabitethernet1       00:45:46/00:01:42  v2    1 / DR

PE1#show ip pim neighbor vrf 2
PIM Neighbor Table:
PIM VRF Name: 2
Total 2 Neighbor entry

Neighbor        Interface              Uptime/Expires     Ver   DR
Address                                                        Priority/Mode
3.3.3.3         tunnel1022             00:20:08/never     v2    N / DR
15.1.1.2        gigabitethernet0/2/2   00:37:21/00:01:37  v2    1 / DR
```

You can see that PE1 sets up the PIM-SM neighbor with CE1, CE2, and sets up the PIM-SM neighbor with the MVPN tunnel interface of the peer PE via the MVPN tunnel interface.

**Note:**

- For the checking method of PE2, refer to PE1.

#On PE, query the P2MP-TE S2L tunnel information.

Take PE1 as an example:

```
PE1#show mpls traffic-eng p2mp summary
P2MP_1.1.1.1_t2
 Role: root         S2L count: 1
 vrf: 1
 S2L tunnel table:
  Name          S2L-Role     LSP-ID    Status  Out-LB  Out-IF                  In-
LB  In-IF
```

```
 S2L-3.3.3.3       Ingress      5        UP     16     gigabitethernet0              N/A
N/A


P2MP_1.1.1.1_t3
 Role: root         S2L count: 1
 vrf: 2
 S2L tunnel table:
 Name              S2L-Role     LSP-ID    Status  Out-LB  Out-IF                    In-
LB  In-IF
 S2L-3.3.3.3       Ingress      6        UP     17     gigabitethernet0              N/A
N/A
```

You can see that the status of the P2MP-TE S2L tunnel from PE1 to PE2 is up.

**Note:**

- For the checking method of P and PE2, refer to PE1.

#Receiver1 is added to IGMPv3 group 225.0.0.1, and is specified to receive the multicast flow sent by the multicast source Source1 and Source2.

Receiver2 is added to IGMPv3 group 226.0.0.1, and is specified to receive the multicast flow sent by the multicast source Source1 and Source2.

On CE3 and CE4, query the IGMP group and PIM-SM route table.

```
CE3#show ip igmp groups detail
Interface: gigabitethernet1
Group:        225.0.0.1
Uptime:       00:00:10
Group mode:    Include
Last reporter:  60.1.1.2
TIB-A Count:    2
TIB-B Count:    0
Group source list: (R - Remote, M - SSM Mapping)
  Source Address  Uptime   v3 Exp    M Exp    Fwd  Flags
  40.1.1.2        00:00:10  00:04:14  stopped   Yes  R
  50.1.1.2        00:00:10  00:04:14  stopped   Yes  R


CE4#show ip igmp groups detail
Interface: gigabitethernet1
Group:        226.0.0.1
Uptime:       00:00:10
Group mode:    Include
Last reporter:  70.1.1.2
```

```
TIB-A Count:    2
TIB-B Count:    0
Group source list: (R - Remote, M - SSM Mapping)
  Source Address  Uptime    v3 Exp    M Exp     Fwd  Flags
  40.1.1.2        00:00:10  00:04:14  stopped   Yes  R
  50.1.1.2        00:00:10  00:04:14  stopped   Yes  R

CE3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 2 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(40.1.1.2, 225.0.0.1)
Up time: 00:03:20
KAT time: 00:00:10
RPF nbr: 36.1.1.1
RPF idx: gigabitethernet0
SPT bit: FALSE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    gigabitethernet1
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 0

(50.1.1.2, 225.0.0.1)
Up time: 00:03:20
```

KAT time: 00:00:10
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: FALSE
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
  gigabitethernet1
 Joined interface list:
 Asserted interface list:
 Outgoing interface list:
  gigabitethernet1
 Packet count 0

CE4#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 2 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer

(40.1.1.2, 226.0.0.1)
Up time: 00:03:20
KAT time: 00:00:10
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: FALSE
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
  gigabitethernet1

```
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 0

(50.1.1.2, 226.0.0.1)
Up time: 00:03:20
KAT time: 00:00:10
RPF nbr: 37.1.1.1
RPF idx: gigabitethernet0
SPT bit: FALSE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    gigabitethernet1
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 0
```

You can see that the group is added on CE3 and CE4 successfully, and the (S,G) route is generated. CE3 and CE2 are not in one VPN, and there is no unicast route to Source2, so only send the (S,G) route to Source1. CE4 is similar.

#On the PE, view the BGP MVPN type-7 route table.

```
PE1#show ip bgp mvpn rd 100:1 type 7
BGP local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
MVPN Information for Route Distinguisher:100:1 (Default for VRF 1)
 Source Tree Join Routes:
     Network(AS Number:C-S:C-G)     Next Hop          Metric     LocPrf Weight Path
[B]*>i100:40.1.1.2:225.0.0.1        3.3.3.3                0       100      0 i

PE1#show ip bgp mvpn rd 200:1 type 7
BGP local router ID is 1.1.1.1
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
MVPN Information for Route Distinguisher:200:1 (Default for VRF 2)
 Source Tree Join Routes:
    Network(AS Number:C-S:C-G)     Next Hop          Metric    LocPrf Weight Path
[B]*>i100:50.1.1.2:226.0.0.1        3.3.3.3              0       100      0 i

PE2#show ip bgp mvpn rd 100:1 type 7
BGP local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
MVPN Information for Route Distinguisher:100:1
 Source Tree Join Routes:
    Network(AS Number:C-S:C-G)     Next Hop          Metric    LocPrf Weight Path
[B]*> 100:40.1.1.2:225.0.0.1        0.0.0.0              0          32768 i

PE2#show ip bgp mvpn rd 200:1 type 7
BGP local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
MVPN Information for Route Distinguisher:200:1
 Source Tree Join Routes:
    Network(AS Number:C-S:C-G)     Next Hop          Metric    LocPrf Weight Path
[B]*> 100:50.1.1.2:226.0.0.1        0.0.0.0              0          32768 i
```

#On PE, query the PIM-SM route table of VPN.

```
PE1#show ip pim mroute vrf 1
IP Multicast Routing Table:
PIM VRF Name: 1
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer
```

(40.1.1.2, 225.0.0.1)
Up time: 00:02:50
KAT time: 00:00:40
RPF nbr: 14.1.1.2
RPF idx: gigabitethernet1
SPT bit: FALSE
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
 Joined interface list:
  tunnel1023  00:02:50/stopped
 Asserted interface list:
 Outgoing interface list:
  tunnel1023
 Packet count 0

PE1#show ip pim mroute vrf 2
IP Multicast Routing Table:
PIM VRF Name: 2
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer

(50.1.1.2, 226.0.0.1)
Up time: 00:02:55
KAT time: 00:00:35
RPF nbr: 15.1.1.2
RPF idx: gigabitethernet0/2/2
SPT bit: FALSE
Flags:

```
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    tunnel1022  00:02:55/stopped
  Asserted interface list:
  Outgoing interface list:
    tunnel1022
  Packet count 0

PE2#show ip pim mroute vrf 1
IP Multicast Routing Table:
PIM VRF Name: 1
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(40.1.1.2, 225.0.0.1)
Up time: 00:03:20
KAT time: 00:00:10
RPF nbr: 1.1.1.1
RPF idx: tunnel1023
SPT bit: FALSE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    gigabitethernet1  00:03:20/00:02:10
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 0
```

```
PE2#show ip pim mroute vrf 2
IP Multicast Routing Table:
PIM VRF Name: 2
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(50.1.1.2, 226.0.0.1)
Up time: 00:03:20
KAT time: 00:00:10
RPF nbr: 1.1.1.1
RPF idx: tunnel1022
SPT bit: FALSE
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
 Joined interface list:
  gigabitethernet0/2/2  00:03:20/00:02:10
 Asserted interface list:
 Outgoing interface list:
  gigabitethernet0/2/2
 Packet count 0
```

You can see that both PE1 and PE2 have the corresponding multicast route, and the egress interface information is correct. Source1 and Source2 send the corresponding multicast flow. Receiver1 can only receive the multicast flow sent by Source1, and Receiver2 can only receive the multicast flow sent by Source2.

**Note:**

- For the checking method of CE1 and CE2, refer to PE1.

### 8.3.3. Configure S-PMSI Tunnel Switching

#### Network Requirements

- There is one MVPN:VPN1 in the network; CE1, CE2 and CE3 belong to VPN1.
- OSPF is used for private unicast routing announcement between CE and PE.

- OSPF is used as IGP in the autonomous domain to realize the interworking between PEs, and MP-IBGP is configured between PEs to exchange unicast VPN routing information.
- VPN1 uses mLDP P2MP as public network I-PMSI and S-PMSI tunnels.
- VPN1 uses PIM-SM as the multicast routing protocol.
- The interfaces of CE2 and CE3 directly connected to the multicast receiver run igmpv3. Receiver1 joins the corresponding multicast group, and receiver2 does not join the corresponding multicast group.
- Source sends the multicast flow. Before the multicast data flow is switched from the I-PMSI tunnel to the S-PMSI tunnel, both Receiver 1 and PE3 can receive the multicast flow; After the multicast data flow is switched from the I-PMSI tunnel to the S-PMSI tunnel, Receiver 1 can receive the multicast flow, but PE3 cannot receive the multicast flow.

## Network Topology

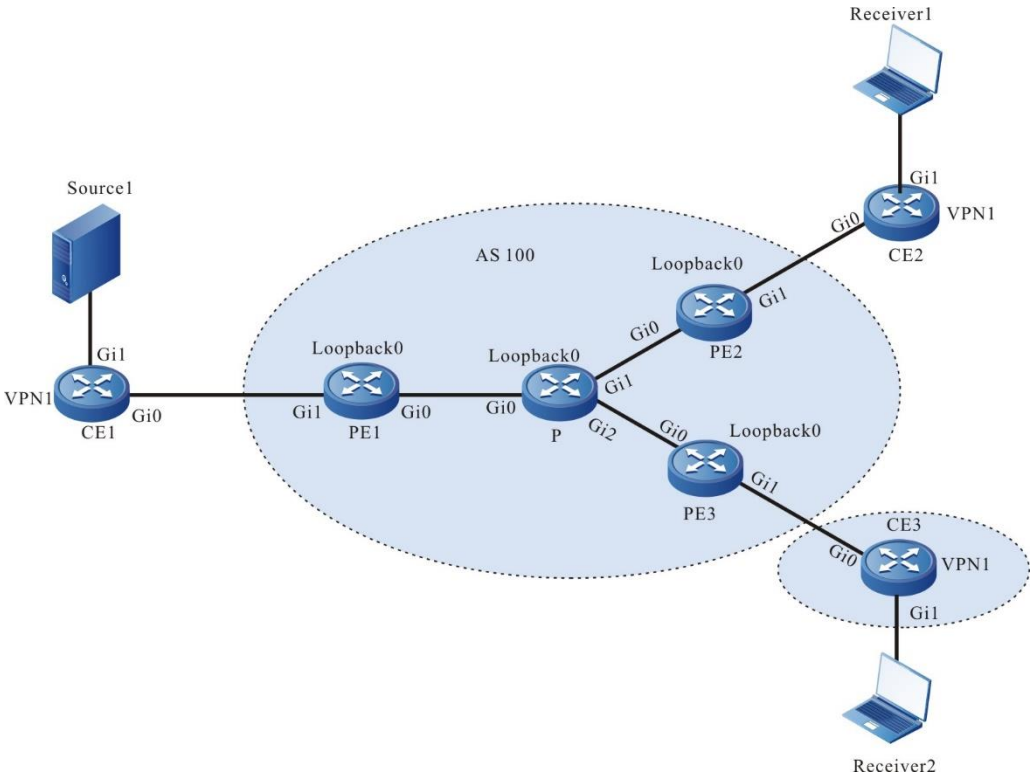


Figure 8-3 Networking of configuring S-PMSI tunnel switching

| Device | Interface | IP address | Device | Interface | IP address |
|---|---|---|---|---|---|
| CE1 | Gi0 | 14.1.1.2/16 | PE2 | Loopback0 | 3.3.3.3/32 |
| | Gi1 | 40.1.1.1/16 | PE3 | Gi0 | 24.1.2.2/16 |
| PE1 | Gi0 | 12.1.1.1/16 | | Gi1 | 37.1.1.1/16 |

| Device | Interface | IP address | Device | Interface | IP address |
|---|---|---|---|---|---|
| | Gi1 | 14.1.1.1/16 | | Loopback0 | 4.4.4.4/32 |
| | Loopback0 | 1.1.1.1/32 | CE2 | Gi0 | 36.1.1.2/16 |
| P | Gi0 | 12.1.1.2/16 | | Gi1 | 60.1.1.1/16 |
| | Gi1 | 23.1.1.1/16 | CE3 | Gi0 | 37.1.1.2/16 |
| | Gi2 | 24.1.2.1/16 | | Gi1 | 70.1.1.1/16 |
| | Loopback0 | 2.2.2.2/32 | Source1 | | 40.1.1.2/16 |
| PE2 | Gi0 | 23.1.1.2/16 | Receiver1 | | 60.1.1.2/16 |
| | Gi1 | 36.1.1.1/16 | Receiver2 | | 70.1.1.2/16 |

## Configuration Steps

**Step 1:** Configure the IP addresses of the interfaces. (omitted)

**Step 2:** Configure global OSPF, and advertise the global route.

#On PE1, configure the global OSPF.

```
PE1#configure terminal
PE1(config)#router ospf 100
PE1(config-ospf)#network 1.1.1.1 0.0.0.0 area 0
PE1(config-ospf)#network 12.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#On P, configure the global OSPF.

```
P#configure terminal
P(config)#router ospf 100
P(config-ospf)#network 2.2.2.2 0.0.0.0 area 0
P(config-ospf)#network 12.1.0.0 0.0.255.255 area 0
P(config-ospf)#network 23.1.0.0 0.0.255.255 area 0
P(config-ospf)#network 24.1.0.0 0.0.255.255 area 0
P(config-ospf)#exit
```

#On PE2, configure global OSPF.

```
PE2#configure terminal
PE2(config)#router ospf 100
PE2(config-ospf)#network 3.3.3.3 0.0.0.0 area 0
PE2(config-ospf)#network 23.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#On PE3, configure global OSPF.

```
PE3#configure terminal
PE3(config)#router ospf 100
PE3(config-ospf)#network 4.4.4.4 0.0.0.0 area 0
PE3(config-ospf)#network 24.1.0.0 0.0.255.255 area 0
PE3(config-ospf)#exit
```

#After configuration, view the global route table on the device.

Take PE1 as an example:

```
PE1#show ip route

Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management

    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   12.1.0.0/16 is directly connected, 00:23:28, gigabitethernet0
O   23.1.0.0/16 [110/2] via 12.1.1.2, 00:01:12, gigabitethernet0
C   1.1.1.1/32 is directly connected, 00:32:21, loopback0
O   2.2.2.2/32 [110/2] via 12.1.1.2, 00:01:12, gigabitethernet0
O   3.3.3.3/32 [110/3] via 12.1.1.2, 00:01:05, gigabitethernet0
O   4.4.4.4/32 [110/3] via 12.1.1.2, 00:01:05, gigabitethernet0
```

It can be seen that the global routing table of PE1 contains the routing information of the loopback ports of P, PE2 and PE3.

**Note:**

- For the checking method of P, PE1 and PE3, refer to PE1.

**Step 3:** Enable MVPN, MPLS IP and MPLS LDP (containing mLDP P2MP).

#Enable global MVPN, MPLS IP and MPLS LDP (including mLDP P2MP) on PE1, and enable MPLS IP and MPLS LDP on the interface at the same time.

```
PE1(config)#mvpn-id 1.1.1.1
PE1(config)#mpls ip
PE1(config)#mpls ldp
PE1(config-ldp)#router-id 1.1.1.1
PE1(config-ldp)#transport-address 1.1.1.1
PE1(config-ldp)#mldp p2mp
PE1(config-ldp)#exit
PE1(config)#interface gigabitethernet0
PE1(config-if-gigabitethernet0)#mpls ip
PE1(config-if-gigabitethernet0)#mpls ldp
PE1(config-if-gigabitethernet0)#exit
```

#Enable the global MPLS IP and MPLS LDP (including mLDP P2MP) on the P, and enable the MPLS IP and MPLS LDP on the interface at the same time.

```
P(config)#mpls ip
P(config)#mpls ldp
P(config-ldp)#router-id 2.2.2.2
P(config-ldp)#transport-address 2.2.2.2
P(config-ldp)#mldp p2mp
P(config-ldp)#exit
P(config)#interface gigabitethernet0
P(config-if-gigabitethernet0)#mpls ip
P(config-if-gigabitethernet0)#mpls ldp
P(config-if-gigabitethernet0)#exit
P(config)#interface gigabitethernet1
P(config-if-gigabitethernet1)#mpls ip
P(config-if-gigabitethernet1)#mpls ldp
P(config-if-gigabitethernet1)#exit
P(config)#interface gigabitethernet 2
P(config-if-gigabitethernet 2)#mpls ip
P(config-if-gigabitethernet 2)#mpls ldp
P(config-if-gigabitethernet 2)#exit
```

#Enable the global MVPN, MPLS IP and MPLS LDP (including mLDP P2MP) on the PE2, and enable the MPLS IP and MPLS LDP on the interface at the same time.

```
PE2(config)#mvpn-id 3.3.3.3
PE2(config)#mpls ip
PE2(config)#mpls ldp
PE2(config-ldp)#router-id 3.3.3.3
PE2(config-ldp)#transport-address 3.3.3.3
```

```
PE2(config-ldp)#mldp p2mp
PE2(config-ldp)#exit
PE2(config)#interface gigabitethernet0
PE2(config-if-gigabitethernet0)#mpls ip
PE2(config-if-gigabitethernet0)#mpls ldp
PE2(config-if-gigabitethernet0)#exit
```

#Enable the global MVPN, MPLS IP and MPLS LDP (including mLDP P2MP) on the PE3, and enable the MPLS IP and MPLS LDP on the interface at the same time.

```
PE3(config)#mvpn-id 4.4.4.4
PE3(config)#mpls ip
PE3(config)#mpls ldp
PE3(config-ldp)#router-id 4.4.4.4
PE3(config-ldp)#transport-address 4.4.4.4
PE3(config-ldp)#mldp p2mp
PE3(config-ldp)#exit
PE3(config)#interface gigabitethernet0
PE3(config-if-gigabitethernet0)#mpls ip
PE3(config-if-gigabitethernet0)#mpls ldp
PE3(config-if-gigabitethernet0)#exit
```

**Note:**

- router-id and transport-address can be configured manually or generated automatically. Generally, they are configured to be the same. If router-id and transport-address are not configured manually, the device will select them automatically. From the interfaces in the up state, first select the largest IP address in the loopback interface; If the loopback interface address is not configured for the device, the largest IP address in the normal interface will be selected.

#After configuration, view the MVPN information on the device.

Take PE1 as an example:

```
PE1#show ip mvpn

 mvpn-id: 1.1.1.1
```

You can see that the MVPN ID of PE1 is 1.1.1.1.

#On the device, view the LDP and mLDP session information.

Take PE1 as an example:

```
PE1#show mpls ldp session
Peer IP Address   Peer Type    My Role   State        DeadTime
2.2.2.2           Multicast    Active    OPERATIONAL  00:02:20
Statistics for ldp sessions:
    Multicast sessions: 1
```

```
Targeted sessions: 0


PE1#show mpls ldp p2mp session
Session[2.2.2.2]:
    P2MP Capability: enable
    MBB Capability: disable
    Nexthop selected: 12.1.1.2
    Nexthop interface selected: gigabitethernet0
```

It can be seen that PE1 and P have successfully established an LDP session, and the LDP session has the P2MP capability.

**Note:**

- For the checking method of P, PE1 and PE3, refer to PE1.

**Step 4:** Configure VPN instance, enable MVPN and multicast forwarding of VRF, and announce CE route to PE through OSPF.

#Configure the VPN instance on PE1 to enable MVPN and multicast forwarding, configure the I-PMSI tunnel type as mLDP P2MP, configure the S-PMSI group range as 225.0.0.0/24, and the tunnel type as mLDP P2MP, and configure PIM-SM and OSPF under VPN1.

```
PE1(config)#ip vrf 1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#address-family ipv4
PE1(config-vrf-ipv4)#mvpn
PE1(config-vrf-ipv4-mvpn)#i-pmsi mldp p2mp
PE1(config-vrf-ipv4-mvpn)#s-pmsi group 225.0.0.0 24 mldp p2mp
PE1(config-vrf-ipv4-mvpn)#exit
PE1(config-vrf-ipv4)#exit
PE1(config-vrf)#exit
PE1(config)#ip multicast-routing vrf 1
PE1(config)#interface gigabitethernet1
PE1(config-if-gigabitethernet1)#ip vrf forwarding 1
PE1(config-if-gigabitethernet1)#ip address 14.1.1.1 255.255.0.0
PE1(config-if-gigabitethernet1)#ip pim sparse-mode
PE1(config-if-gigabitethernet1)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#network 14.1.0.0 0.0.255.255 area 0
PE1(config-ospf)#exit
```

#On CE1, enable the multicast forwarding, and configure PIM-SM and OSPF.

```
CE1(config)#ip multicast-routing
CE1(config)#interface gigabitethernet0
CE1(config-if-gigabitethernet0)#ip pim sparse-mode
CE1(config-if-gigabitethernet0)#exit
CE1(config)#interface gigabitethernet1
CE1(config-if-gigabitethernet1)#ip pim sparse-mode
CE1(config-if-gigabitethernet1)#exit
CE1(config)#router ospf 100
CE1(config-ospf)#network 14.1.0.0 0.0.255.255 area 0
CE1(config-ospf)#network 40.1.0.0 0.0.255.255 area 0
CE1(config-ospf)#exit
```

#Configure VPN instance on PE2 to enable MVPN and multicast forwarding, and configure PIM-SM and OSPF under VPN1.

```
PE2(config)#ip vrf 1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target export 100:1
PE2(config-vrf)#route-target import 100:1
PE2(config-vrf)#address-family ipv4
PE2(config-vrf-ipv4)#mvpn
PE2(config-vrf-ipv4-mvpn)#exit
PE2(config-vrf-ipv4)#exit
PE2(config-vrf)#exit
PE2(config)#ip multicast-routing vrf 1
PE2(config)#interface gigabitethernet1
PE2(config-if-gigabitethernet1)#ip vrf forwarding 1
PE2(config-if-gigabitethernet1)#ip address 36.1.1.1 255.255.0.0
PE2(config-if-gigabitethernet1)#ip pim sparse-mode
PE2(config-if-gigabitethernet1)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#network 36.1.0.0 0.0.255.255 area 0
PE2(config-ospf)#exit
```

#Enable multicast forwarding on CE2, configure PIM-SM and OSPF, and configure IGMPv3 on the interface connecting the multicast receiver.

```
CE2(config)#ip multicast-routing
CE2(config)#interface gigabitethernet0
CE2(config-if-gigabitethernet0)#ip pim sparse-mode
CE2(config-if-gigabitethernet0)#exit
```

```
CE2(config)#interface gigabitethernet1
CE2(config-if-gigabitethernet1)#ip pim sparse-mode
CE2(config-if-gigabitethernet1)#ip igmp version 3
CE2(config-if-gigabitethernet1)#exit
CE2(config)#router ospf 100
CE2(config-ospf)#network 36.1.0.0 0.0.255.255 area 0
CE2(config-ospf)#network 60.1.0.0 0.0.255.255 area 0
CE2(config-ospf)#exit
```

#Configure VPN instance on PE3, enable MVPN and multicast forwarding, and configure PIM-SM and OSPF under VPN1.

```
PE3(config)#ip vrf 1
PE3(config-vrf)#rd 100:1
PE3(config-vrf)#route-target export 100:1
PE3(config-vrf)#route-target import 100:1
PE3(config-vrf)#address-family ipv4
PE3(config-vrf-ipv4)#mvpn
PE3(config-vrf-ipv4-mvpn)#exit
PE3(config-vrf-ipv4)#exit
PE3(config-vrf)#exit
PE3(config)#ip multicast-routing vrf 1
PE3(config)#interface gigabitethernet1
PE3(config-if-gigabitethernet1)#ip vrf forwarding 1
PE3(config-if-gigabitethernet1)#ip address 37.1.1.1 255.255.0.0
PE3(config-if-gigabitethernet1)#ip pim sparse-mode
PE3(config-if-gigabitethernet1)#exit
PE3(config)#router ospf 200 vrf 1
PE3(config-ospf)#network 37.1.0.0 0.0.255.255 area 0
PE3(config-ospf)#exit
```

#Enable multicast forwarding on CE3, configure PIM-SM and OSPF, and configure IGMPv3 on the interface connecting the multicast receiver.

```
CE3(config)#ip multicast-routing
CE3(config)#interface gigabitethernet0
CE3(config-if-gigabitethernet0)#ip pim sparse-mode
CE3(config-if-gigabitethernet0)#exit
CE3(config)#interface gigabitethernet1
CE3(config-if-gigabitethernet1)#ip pim sparse-mode
CE3(config-if-gigabitethernet1)#ip igmp version 3
CE3(config-if-gigabitethernet1)#exit
```

```
CE3(config)#router ospf 100
CE3(config-ospf)#network 37.1.0.0 0.0.255.255 area 0
CE3(config-ospf)#network 70.1.0.0 0.0.255.255 area 0
CE3(config-ospf)#exit
```

#On PE, view the VPN route table and PIM-SM interface information.

Take PE1 as an example:

```
PE1#show ip route vrf 1
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   14.1.0.0/16 is directly connected, 00:11:45, gigabitethernet1
O   40.1.0.0/16 [110/2] via 14.1.1.2, 00:11:11, gigabitethernet1

PE1#show ip pim interface vrf 1
PIM Interface Table:
PIM VRF Name: 1
Total 2 Interface entries
Total 1 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address       Interface              VIF    Ver/  VIF  Nbr   DR   DR        BSR
CISCO   Neighbor
                                     Index  Mode  Flag Count Pri            Border
Neighbor Filter
14.1.1.1      gigabitethernet1       0      v2/S  UP   1     1    14.1.1.2  FALSE FALSE
0.0.0.0       tunnel1023             2      v2/S  UP   0     1    0.0.0.0   FALSE
FALSE
```

It can be seen that there is a route to CE1 in the VPN1 routing table of PE1. The PIM-SM interface table includes the enabled PIM-SM interface and the automatically generated MVPN tunnel interface.

**Note:**

- For the checking method of PE2, PE3, CE2, and CE3, refer to PE1.
- The PE on the multicast source side must be configured with a tunnel type, and the PE on the multicast receiving side may not be configured with a tunnel type.
- Tunnel 1023 is an MVPN interface. When MVPN is enabled for global and VRF, each VPN will automatically generate a tunnel interface.

**Step 5:** Configure MP-IBGP and use the loopback interface as the peer address; and redistribute the route with the IGP protocol under the VPN instance.

#Configure MP-IBGP on PE1 and enable VPNv4 and IPv4 MVPN address families; And redistribute the route with the IGP protocol under the VPN instance.

```
PE1(config)#router bgp 100
PE1(config-bgp)#neighbor 3.3.3.3 remote-as 100
PE1(config-bgp)#neighbor 3.3.3.3 update-source loopback0
PE1(config-bgp)#neighbor 4.4.4.4 remote-as 100
PE1(config-bgp)#neighbor 4.4.4.4 update-source loopback0
PE1(config-bgp)#address-family vpnv4
PE1(config-bgp-af)#neighbor 3.3.3.3 activate
PE1(config-bgp-af)#neighbor 4.4.4.4 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 mvpn
PE1(config-bgp-af)#neighbor 3.3.3.3 activate
PE1(config-bgp-af)#neighbor 4.4.4.4 activate
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#address-family ipv4 vrf 1
PE1(config-bgp-af)#redistribute ospf 200
PE1(config-bgp-af)#exit-address-family
PE1(config-bgp)#exit
PE1(config)#router ospf 200 vrf 1
PE1(config-ospf)#redistribute bgp 100
PE1(config-ospf)#exit
```

#Configure MP-IBGP on PE2 and enable VPNv4 and IPv4 MVPN address families; And redistribute the route with the IGP protocol under the VPN instance.

```
PE2(config)#router bgp 100
PE2(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-bgp)#neighbor 1.1.1.1 update-source loopback0
PE2(config-bgp)#address-family vpnv4
PE2(config-bgp-af)#neighbor 1.1.1.1 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 mvpn
PE2(config-bgp-af)#neighbor 1.1.1.1 activate
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#address-family ipv4 vrf 1
PE2(config-bgp-af)#redistribute ospf 200
```

```
PE2(config-bgp-af)#exit-address-family
PE2(config-bgp)#exit
PE2(config)#router ospf 200 vrf 1
PE2(config-ospf)#redistribute bgp 100
PE2(config-ospf)#exit
```

#Configure MP-IBGP on PE3 and enable VPNv4 and IPv4 MVPN address families; And redistribute the route with the IGP protocol under the VPN instance.

```
PE3(config)#router bgp 100
PE3(config-bgp)#neighbor 1.1.1.1 remote-as 100
PE3(config-bgp)#neighbor 1.1.1.1 update-source loopback0
PE3(config-bgp)#address-family vpnv4
PE3(config-bgp-af)#neighbor 1.1.1.1 activate
PE3(config-bgp-af)#exit-address-family
PE3(config-bgp)#address-family ipv4 mvpn
PE3(config-bgp-af)#neighbor 1.1.1.1 activate
PE3(config-bgp-af)#exit-address-family
PE3(config-bgp)#address-family ipv4 vrf 1
PE3(config-bgp-af)#redistribute ospf 200
PE3(config-bgp-af)#exit-address-family
PE3(config-bgp)#exit
PE3(config)#router ospf 200 vrf 1
PE3(config-ospf)#redistribute bgp 100
PE3(config-ospf)#exit
```

**Note:**

- In the practical application, if there are two or more PE devices on the same site side, it is recommended not to redistribute routes directly between different routing protocols. If it must be configured, it is necessary to configure routing policies to prevent routing loops.

**Step 6:** Check the result.

#After configuration, view the BGP neighbor information on the PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
```

```
3.3.3.3         4  100     40     41      6    0    0 00:32:01        4
4.4.4.4         4  100     40     41      6    0    0 00:32:01        4

Total number of neighbors 2
PE1#show ip bgp mvpn summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
3.3.3.3         4  100     527     539        6    0    0 00:03:32        2
4.4.4.4         4  100     527     539        6    0    0 00:03:32        2

Total number of neighbors 2
```

From the contents of the State/PfxRcd column displayed as numbers (the number of routing prefixes received from neighbors), it can be seen that PE1 and PE2 successfully established BGP neighbors.

#View the BGP VPNv4 routing table, BGP MVPN routing table and VPN routing table on PE.

Take PE1 as an example:

```
PE1#show ip bgp vpnv4 vrf 1
BGP table version is 6, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (Default for VRF 1)
[0]*> 14.1.0.0/16    0.0.0.0                  1         32768 ?
[0]*> 40.1.0.0/16    14.1.1.2                 2         32768 ?
[B]*>i36.1.0.0/16    3.3.3.3                  1    100      0 ?
[B]*>i60.1.0.0/16    3.3.3.3                  2    100      0 ?
[B]*>i37.1.0.0/16    4.4.4.4                  1    100      0 ?
[B]*>i70.1.0.0/16    4.4.4.4                  2    100      0 ?


PE1#show ip bgp mvpn vrf 1 all-type
BGP local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
MVPN Information for Route Distinguisher:100:1 (Default for VRF 1)
 Intra-AS I-PMSI A-D Routes:
    Network(Originating IP Addr)   Next Hop        Metric    LocPrf Weight Path
[B]*> 1.1.1.1                    0.0.0.0           0         32768 i
[B]*>i3.3.3.3                     3.3.3.3           0      100     0 i
[B]*>i4.4.4.4                     4.4.4.4           0      100     0 i

PE1#show ip route vrf 1
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M -
Management
     D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B   36.1.0.0/16 [200/1] via 3.3.3.3, 00:01:06, gigabitethernet0
B   37.1.0.0/16 [200/1] via 4.4.4.4, 00:01:06, gigabitethernet0
C   14.1.0.0/16 is directly connected, 00:23:25, gigabitethernet1
O   40.1.0.0/16 [110/2] via 14.1.1.2, 00:22:51, gigabitethernet1
B   60.1.0.0/16 [200/2] via 3.3.3.3, 00:01:06, gigabitethernet0
B   70.1.0.0/16 [200/2] via 4.4.4.4, 00:01:06, gigabitethernet0
```

You can see that the routing information to the peer CE2 and CE3 exists under the BGP VPNv4routing table and VPN1 routing table of PE1. There is class-1 MVPN routing information advertised by peer PE2 and PE3 under the BGP MVPN routing table of PE1.

#View PIM-SM neighbor information on PE.

Take PE1 as an example:

```
PE1#show ip pim neighbor vrf 1
PIM Neighbor Table:
PIM VRF Name: 1
Total 3 Neighbor entry

Neighbor        Interface              Uptime/Expires     Ver   DR
Address                                                        Priority/Mode
3.3.3.3         tunnel1023             00:19:51/never     v2    N /
4.4.4.4         tunnel1023             00:19:51/never     v2    N / DR
14.1.1.2        gigabitethernet1       00:45:46/00:01:42  v2    1 / DR
```

It can be seen that PE1 and CE1 establish PIM-SM neighbors, and establish PIM-SM neighbors with the MVPN tunnel interfaces of peer PE2 and PE3 through the MVPN tunnel interface.

**Note:**

- For the checking methods of PE2 and PE3, refer to PE1.

For the checking methods of PE2 and PE3, refer to PE1.#Receiver1 joins IGMPv3 group 225.0.0.1 and specifies to receive the multicast flow sent by multicast source source1. Receiver2 does not join the multicast group 225.0.0.1.

#View the grouping information and multicast routing table on CE2 and CE3.

```
CE2#show ip igmp groups detail
Interface: gigabitethernet1
Group:         225.0.0.1
Uptime:        00:00:10
Group mode:    Include
Last reporter: 60.1.1.2
TIB-A Count:   1
TIB-B Count:   0
Group source list: (R - Remote, M - SSM Mapping)
  Source Address  Uptime    v3 Exp    M Exp     Fwd  Flags
  40.1.1.2        00:00:10  00:04:14  stopped   Yes  R

CE2#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(40.1.1.2, 225.0.0.1)
Up time: 00:03:20
KAT time: 00:00:10
RPF nbr: 36.1.1.1
RPF idx: gigabitethernet0
SPT bit: FALSE
Flags:
```

```
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    gigabitethernet1
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 0


CE3#show ip igmp groups detail


CE3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 0 (S,G) entry
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer
```

It can be seen that CE2 adds groups successfully, and CE2 generates corresponding (S, G) routes; CE3 does not add groups, and CE3 does not generate (S, G) routes.

#View the multicast routing table on PE2 and PE3.

```
PE2#show ip pim mroute vrf 1
IP Multicast Routing Table:
PIM VRF Name: 1
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer



(40.1.1.2, 225.0.0.1)
Up time: 00:03:20
```

```
KAT time: 00:00:10
RPF nbr: 1.1.1.1
RPF idx: tunnel1023
SPT bit: FALSE
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
 Joined interface list:
  gigabitethernet1  00:03:20/00:02:10
 Asserted interface list:
 Outgoing interface list:
  gigabitethernet1
 Packet count 0

PE3#show ip pim mroute vrf 2
IP Multicast Routing Table:
PIM VRF Name: 2
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 0 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer
```

It can be seen that PE2 generates corresponding (S, G) routes, while PE3 does not generate (S, G) routes.

#View BGP MVPN class-7 routing table on PE.

```
PE1#show ip bgp mvpn rd 100:1 type 7
BGP local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
MVPN Information for Route Distinguisher:100:1 (Default for VRF 1)
 Source Tree Join Routes:
     Network(AS Number:C-S:C-G)     Next Hop          Metric     LocPrf Weight Path
[B]*>i100:40.1.1.2:225.0.0.1        3.3.3.3              0       100      0 i
```

```
PE2#show ip bgp mvpn rd 100:1 type 7
BGP local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
MVPN Information for Route Distinguisher:100:1
 Source Tree Join Routes:
    Network(AS Number:C-S:C-G)     Next Hop          Metric     LocPrf Weight Path
[B]*> 100:40.1.1.2:225.0.0.1        0.0.0.0               0          32768 i

PE3#show ip bgp mvpn rd 100:1 type 7
```

It can be seen that PE1 and PE2 have corresponding class-7 MVPN routes, and PE3 has no corresponding class-7 MVPN routes.

#View the multicast routing table on PE1.

```
PE1#show ip pim mroute vrf 1
IP Multicast Routing Table:
PIM VRF Name: 1
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(40.1.1.2, 225.0.0.1)
Up time: 00:02:50
KAT time: 00:00:40
RPF nbr: 14.1.1.2
RPF idx: gigabitethernet1
SPT bit: FALSE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    tunnel1023  00:02:50/stopped
```

```
Asserted interface list:
Outgoing interface list:
 tunnel1023
Packet count 0
```

You can see that PE1 generates corresponding (S, G) routes.

#Source1 continuously sends multicast data flows with source address of 40.1.1.2 and group address of 225.0.0.1.

#View the multicast forwarding table of VPN on PE.

```
PE1# show ip mcache vrf 1
Multicast Forward Cache table:
Total 1 MFC entries
Total 0 stall upcall packet
MFC (40.1.1.2/32,  225.0.0.1/32)
 Incoming interface: gigabitethernet1(0)
 Flags: PROTOCOL IPMC
 Ng-mvpn mfc pmsi index: 1
 Output interface list:
  Tunnel1023(2)
 Waiting packets: NULL
 Uptime: 00:00:53, Timeout in 179 sec

PE1#show ip mvpn s-pmsi mrt vrf 1
VRF: 1 Total 10mrt entry
 source:40.1.1.2
 group:225.0.0.1
  last_bytes:38461570
  Rate: 3683 kbps(100 secs)
  i2s Up time: 00:00:59  i2s Expiry time: 00:01:20
Up time: 00:00:59  Expiry time: 00:02:21

PE2#show ip mcache vrf 1
Multicast Forward Cache table:
Total 1 MFC entries
Total 0 stall upcall packet
MFC (40.1.1.2/32,  225.0.0.1/32)
 Incoming interface: tunnel1023(2)
```

```
Flags: PROTOCOL IPMC
Output interface list:
  gigabitethernet1(0)
Waiting packets: NULL
Uptime: 00:01:31, Timeout in 88 sec

PE3#show ip mcache vrf 1
Multicast Forward Cache table:
Total 1 MFC entries
Total 0 stall upcall packet
MFC (40.1.1.2/32,  225.0.0.1/32)
  Incoming interface: tunnel1023(2)
  Flags: PROTOCOL IPMC
  Output interface list:  NULL
  Waiting packets: NULL
  Uptime: 00:01:31, Timeout in 88 sec
```

It can be seen that there are corresponding multicast forwarding tables in PE1, PE2 and PE3, and the output interface information is correct. Before the multicast data flow sent by source1 is switched from the I-PMSI tunnel to the S-PMSI tunnel, both Receiver 1 and PE3 can receive the multicast flow.

**Note:**

- For the checking methods of CE1 and CE2, refer to PE1.
- The sending PE (PE1) receives the multicast data flow, detects that the traffic of the data stream within the S-PMS group is greater than or equal to the S-PMSI switching threshold (0 by default), starts the I-PMSI to switch to the S-PMSI timer (12s timer for short), and the multicast data flow will not switch to the S-PMSI tunnel before the i2s timer expires; After the I2S timer expires, the data flow is still greater than or equal to the S-PMSI switching threshold, and the S-PMSI tunnel is successfully established, and the data flow is switched to the S-PMSI tunnel.

#After the i2s timer expires, view the multicast forwarding table of VPN on PE.

```
PE1# show ip mcache vrf 1
Multicast Forward Cache table:
Total 1 MFC entries
Total 0 stall upcall packet
MFC (40.1.1.2/32,  225.0.0.1/32)
  Incoming interface: gigabitethernet1(0)
  Flags: PROTOCOL IPMC
  Ng-mvpn mfc pmsi index: 2
  Output interface list:
   Tunnel1023(2)
```

```
  Waiting packets: NULL
  Uptime: 00:00:53, Timeout in 179 sec

PE1#show ip mvpn s-pmsi mrt vrf 1
VRF: 1 Total 10mrt entry
  source:40.1.1.2
  group:225.0.0.1
    last_bytes:362877340
    Rate: 3685 kbps(100 secs)
    pmsi index: 2  ptunnel index: 65537
    Up time: 00:12:10  Expiry time: 00:02:50
PE2#show ip mcache vrf 1
Multicast Forward Cache table:
Total 1 MFC entries
Total 0 stall upcall packet
MFC (40.1.1.2/32,  225.0.0.1/32)
  Incoming interface: tunnel1023(2)
  Flags: PROTOCOL IPMC
  Output interface list:
    gigabitethernet1(0)
  Waiting packets: NULL
  Uptime: 00:01:31, Timeout in 88 sec

PE3#show ip mcache vrf 1
Multicast Forward Cache table:
Total 0 MFC entry
Total 0 stall upcall packet
```

It can be seen that the multicast forwarding table entry of PE1 is correct. After the i2s timer expires, the multicast data flow sent by Source1 on PE1 is switched from the I-PMSI tunnel to the S-PMSI tunnel; PE2 still has corresponding multicast forwarding table entries, and PE3 does not have corresponding multicast forwarding entries (deleted after timeout); After the multicast data flow on PE1 is switched from I-PMSI tunnel to the S-PMSI tunnel, Receiver 1 can receive the multicast flow, and PE3 cannot receive the multicast flow.

# 9. MSDP

## 9.1. Overview

RP in the PIM-SM network only knows the multicast source information in the multicast domain, but in the actual application, the whole network is divided to multiple multicast domains. In the case, the RP in the domain cannot know the multicast source information out of the domain and the receiver cannot receive the multicast packets of other domains.

MSDP (Multicast Source Discovery Protocol) provides one multicast cross-domain solution. The MSDP mechanism transmits the multicast source information of the multicast domain to the RP of another multicast domain, and the RP in the other multicast domain can initiate adding to the multicast source of the multicast domain and set up the multicast distributing tree, so as to realize the cross-domain transmission of the multicast packets.

## 9.2. MSDP Function Configuration

Table 9-1 MSDP function configuration list

| Configuration Task | |
|---|---|
| Configure the MSDP basic functions | Configure the MSDP peer |
| | Disable the MSDP peer |
| Configure the MSDP peer connection | Configure the default MSDP peer |
| | Configure the MSDP mesh group |
| Configure the SA packet | Configure the SA request packet |
| | Configure the SA packet filter policy |

### 9.2.1. Configure MSDP Peer

Set up the MSDP peer connection via the MSDP peer between the multicast domains, forming one “MSDP interconnection map”. When the MSDP peer of one domain perceives the new multicast source, encapsulate the new multicast source information in the SA (Source-Active) packet and send to all remote peers setting up the MSDP peer connection. After MSDP peer receives the SA packet, the SA packet passing the RPF (Reverse Path Forwarding) is forwarded. With the relay between the MSDP peers, you can transmit the SA message sent by one RP to all the other RPs, realizing the sharing of the multicast source information between the multicast domains.

Use the TCP as the transmission protocol between the MSDP peers. Use the reliability of TCP to ensure that the MSDP protocol packets can be transmitted to the remote peer correctly.

#### Configuration Condition

Before configuring MSDP, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Configure the PIM-SM protocol, realizing the intra-domain multicast

### Configure MSDP Peer

Set up the MSDP peer connection between the local device and the specified remote device. At the remote device, you also should specify the local device as the MSDP peer so that the peer connection can be set up successfully. After the peer connection is set up successfully, the peers interact the MSDP protocol packets via the connection.

Table 9-2 Configure the MSDP peer

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the MSDP peer | **ip msdp** [ **vrf** *vrf-name* ] **peer** *peer-ip-address* [ **connect-source** *interface-name* ] [ **remote-as** *as-number-value* ] | Mandatory<br>By default, the MSDP peer is not configured. |

**Note:**

- When configuring the first MSDP peer, automatically enable the MSDP protocol.

### Disable MSDP Peer

The administrator can disable the specified MSDP peer connection via the command according to the network demand. After disabling the MSDP peer connection, stop interacting the MSDP protocol packets between the MSDP peers.

Table 9-3 Disable the MSDP peer

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Disable the MSDP peer | **ip msdp** [ **vrf** *vrf-name* ] **shutdown** *peer-ip-address* | Mandatory<br>By default, do not disable the MSDP peer. |

## 9.2.2. Configure MSDP Peer Connection

After the device receives the SA packet, perform the RPF check. The packets passing the check are forwarded to the other peers that set up the peer connection. The packets not passing the RPF check are dropped.

The default peer, mesh group can omit specifying the RPF check of the SA packet between the peers.

### Configuration Condition

Before configuring MSDP, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Configure the PIM-SM protocol, realizing the intra-domain multicast
- Configure the MSDP peer

### Configure Default MSDP Peer

When specifying the default MSDP peer, you can configure the RP range. When receiving the SA packet sent by the default peer and if the RP in the packet belongs to the permitted range, do not perform the RPF check. Otherwise, still perform the RPF check for the RP in the packet.

Table 9-4 Configure the default MSDP peer

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the default MSDP peer | **ip msdp** [ **vrf** *vrf-name* ] **default-peer** *peer-ip-address* [ **prefix-list** *prefix-list-name* ] | Mandatory<br>By default, the MSDP default peer is not configured. |

### Configure MSDP Mesh Group

When receiving the SA packet from the peer in the group, the device directly passes the RPF check and does not forward the SA packet to the other peers in the group, but just forwards to the peers out of the group. This can reduce the load of the device and avoid the repeated forwarding, so as to save the network bandwidth.

Table 9-5 Configure the MSDP mesh group

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the MSDP mesh group | **ip msdp** [ **vrf** *vrf-name* ] **mesh-group** *mesh-group-name peer-ip-address* | Mandatory<br>By default, no peer is added to the mesh group. |

## 9.2.3. Configure SA Packet

### Configuration Condition

Before configuring MSDP, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Configure the PIM-SM protocol, realizing the intra-domain multicast
- Configure the MSDP peer

### Configure SA Request Packet

After configuring the SA request packet on the device, the device immediately sends the SA request packet to MSDP peer when receiving the new multicast group adding packet, so as to reduce the adding delay of the multicast group.

Some RP does not hope to be known by the receivers of the un-recognized other multicast domain. You can configure the filter policy of the SA request packet on all peers of the multicast domain to which the RP belongs. Only answer the SA request packet of the peers permitted by the policy.

Table 9-6 Configure the SA request packet

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure sending the SA request packet | **ip msdp** [ **vrf** *vrf-name* ] **sa-request** *peer-ip-address* | Mandatory<br>By default, when receiving the new multicast group adding packet, the device does not send the SA request packet to the MSDP peer, but waits for the SA packet of the next period. |
| Configure the filter policy of the received SA request packet | **ip msdp** [ **vrf** *vrf-name* ] **filter-sa-request** *peer-ip-address* [ **list** *access-list-number* \| *access-list-name* ] | Mandatory<br>By default, do not filter the SA request packet. |

**Note:**

- **ip msdp filter-sa-request** only supports the standard ACL.

### Configure SA Packet Filter Policy

Usually, the MSDP peer accepts the SA packets from all peers that pass the RPF check and forward to all the peers out of the mesh group. The user can configure the filter policy of the SA packet on the peer as desired, controlling the SA packets from or sent to the specified peer.

When receiving or forwarding the SA packet, the device filters the multicast source group and RP of the SA packet.

Table 9-7 Configure the filter policy of the SA packet

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the filter policy of the SA packet | **ip msdp** [ **vrf** *vrf-name* ] **sa-filter** { **in** \| **out** } *peer-ip-address* [ **list** { *access-list-name* \| *access-list-number* } ] [ **rp-list** { *access-list-name* \| *access-list-number* } ] | Mandatory<br>By default, do not filter the SA packet. |

**Note:**

- The **list** parameter of **ip msdp sa-filter** only supports the extended ACL.
- The **rp-list** parameter of **ip msdp sa-filter** only supports the standard ACL.

### 9.2.4. MSDP Monitoring and Maintaining

Table 9-8 MSDP Monitoring and Maintaining

| Command | Description |
|---|---|
| **clear ip msdp** [ **vrf** *vrf-name* ] **peer** [ *peer-ip-address* ] | Clear the MSDP peer information |
| **clear ip msdp** [ **vrf** *vrf-name* ] **sa-cache** [ *group-ip-address* ] | Clear the SA cache information |
| **clear ip msdp** [ **vrf** *vrf-name* ] **statistics** [ *peer-ip-address* ] | Clear the statistics information of the MSDP peers |
| **show ip msdp** [ **vrf** *vrf-name* ] **count** [ *as-number-value* ] | Display the SA information received by MSDP from the AS domain |
| **show ip msdp** [ **vrf** *vrf-name* ] **peer** [ *peer-ip-address* [ *accepted-SAs* \| *advertised-SAs* ] ] | Display the MSDP peer information |
| **show ip msdp** [ **vrf** *vrf-name* ] **rpf** [ *peer-ip-address* ] | Display the MSDP next-hop route information |

| Command | Description |
|---|---|
| **show ip msdp** [ **vrf** *vrf-name* ] **sa-cache** [ *group-ip-address* [ *source-ip-address* ] ] [ *as-number-value* ] | Display the MSDP SA cache information |
| **show ip msdp** [ **vrf** *vrf-name* ] **summary** | Display the summery information of the MSDP peer |

## 9.3. MSDP Typical Configuration Example

### 9.3.1. Configure Inter-PIM-SM Domain Multicast

#### Network Requirements

- The whole network includes two AS: AS100 and AS200. Run the BGP protocol between Ass and use MBGP to interact the multicast route; in AS, run the OSPF protocol to interact the route.
- Multicast domain PIM-SM1 is located in AS100; multicast domain PIM-SM2 is located in AS200. Source is one multicast source of PIM-SM1. Receiver is one receiver of PIM-SM2.
- Loopback0 and Loopback1 of Device2 are C-BSR and C-RP of PIM-SM1. Loopback0, Loopback1 of Device3 are C-BSR and C-RP of PIM-SM2.
- Between Device2 and Device3, set up the MSDP peer connection, so as to realize the cross-domain forwarding of the multicast service packet, so that Receiver can receive the multicast service packet sent by Source.

#### Network Topology

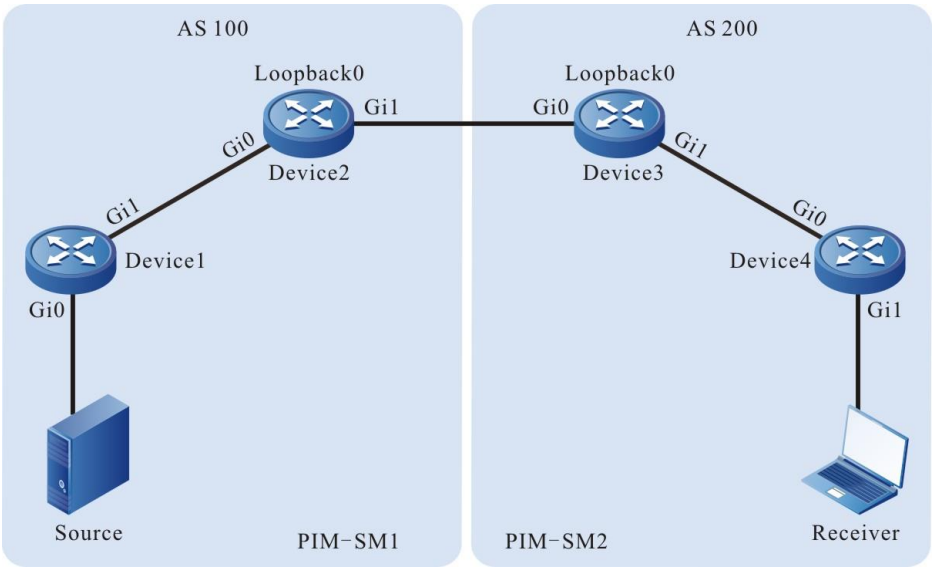


Figure 9-1 Networking of configuring the inter-PIM-SM domain multicast

| Device | Interface | IP address | Device | Interface | IP address |
|---|---|---|---|---|---|
| Device1 | Gi0 | 10.1.1.1/24 | Device3 | Gi0 | 10.1.3.2/24 |
| | Gi1 | 10.1.2.1/24 | | Gi1 | 10.1.4.1/24 |
| Device2 | Gi0 | 10.1.2.2/24 | | Loopback0 | 22.22.22.22/32 |
| | Gi1 | 10.1.3.1/24 | | Loopback1 | 23.23.23.23/32 |
| | Loopback0 | 11.11.11.11/32 | Device4 | Gi0 | 10.1.4.2/24 |
| Source | - | 10.1.1.2/24 | | | |

## Configuration Steps

**Step 1:** Configure the IP address of the interface. (omitted)

**Step 2:** Configure OSPF so that all devices in the AS domain can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device2(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
Device2(config-ospf)#network 12.12.12.12 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
Device3(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
Device3(config-ospf)#network 23.23.23.23 0.0.0.0 area 0
```

```
Device3(config-ospf)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
Device4(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
Device4(config-ospf)#exit
```

#View the route table of Device1.

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.1.1.0/24 is directly connected, 00:05:44, gigabitethernet0
C   10.1.2.0/24 is directly connected, 22:24:35, gigabitethernet1
O   11.11.11.11/32 [110/2] via 10.1.2.2, 01:21:25, gigabitethernet1
12.12.12.12/32 [110/2] via 10.1.2.2, 01:19:25, gigabitethernet1
```

#View the route table of Device4.

```
Device4#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
    D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C   10.1.4.0/24 is directly connected, 22:41:14, gigabitethernet0
C   10.1.5.0/24 is directly connected, 00:08:11, gigabitethernet1
O   22.22.22.22/32 [110/2] via 10.1.4.1, 01:23:33, gigabitethernet0
23.23.23.23/32 [110/2] via 10.1.4.1, 01:19:33, gigabitethernet0
```

You can see that Device1 and Device4 only learn the routes of the belonging AS domain.

**Note:**

- The viewing method of Device2 and Device3 is the same as that of Device1, Device4, so the viewing process is omitted.

**Step 3:** Globally enable the multicast forwarding, enable the multicast protocol PIM-SM on the interface, and configure C-BSR and C-RP.

#Configure Device1.

Globally enable the multicast forwarding, and enable the multicast protocol PIM-SM on the interfaces.

```
Device1(config)#ip multicast-routing
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip pim sparse-mode
Device1(config-if-gigabitethernet0)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#ip pim sparse-mode
Device1(config-if-gigabitethernet1)#exit
```

#Configure Device2.

Globally enable the multicast forwarding, enable the multicast protocol PIM-SM on the interface, configure the BSR border on interface Gigabitethernet1, and configure Loopback1 as C-BSR, and Loopback0 as C-RP; the multicast group range of the C-RP service is 224.0.0.0/4.

```
Device2(config)#ip multicast-routing
Device2(config)#interface loopback 0
Device2(config-if-loopback0)#ip pim sparse-mode
Device2(config-if-loopback0)#exit
Device2(config)#interface loopback 1
Device2(config-if-loopback1)#ip pim sparse-mode
Device2(config-if-loopback1)#exitDevice2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ip pim sparse-mode
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ip pim sparse-mode
Device2(config-if-gigabitethernet1)#ip pim bsr-border
Device2(config-if-gigabitethernet1)#exit
Device2(config)#ip pim bsr-candidate loopback1
Device2(config)#ip pim rp-candidate loopback0
```

#Configure Device3.

Globally enable the multicast forwarding, enable the multicast protocol PIM-SM on the interface, configure the BSR border on interface Gigabitethernet0, and configure Loopback1 as C-BSR, and Loopback0 as C-RP; the multicast group range of the C-RP service is 224.0.0.0/4.

```
Device3(config)#ip multicast-routing
Device3(config)#interface loopback 0
Device3(config-if-loopback0)#ip pim sparse-mode
Device3(config-if-loopback0)#exit
Device3(config)#interface loopback 1
```

```
Device3(config-if-loopback1)#ip pim sparse-mode
Device3(config-if-loopback1)#exitDevice3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#ip pim sparse-mode
Device3(config-if-gigabitethernet0)#ip pim bsr-border
Device3(config-if-gigabitethernet0)#exit
Device3(config)#interface gigabitethernet1
Device3(config-if-gigabitethernet1)#ip pim sparse-mode
Device3(config-if-gigabitethernet1)#exit
Device3(config)#ip pim bsr-candidate loopback1
Device3(config)#ip pim rp-candidate loopback0
```

#Configure Device4.

Globally enable the multicast forwarding, and enable the multicast protocol PIM-SM on the interfaces.

```
Device4(config)#ip multicast-routing
Device4(config)#interface gigabitethernet0
Device4(config-if-gigabitethernet0)#ip pim sparse-mode
Device4(config-if-gigabitethernet0)#exit
Device4(config)#interface gigabitethernet1
Device4(config-if-gigabitethernet1)#ip pim sparse-mode
Device4(config-if-gigabitethernet1)#exit
```

#View the information of the interface enabled with the PIM-SM protocol on Device4 and the PIM-SM neighbor information.

```
Device4#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 3 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address         Interface                VIF     Ver/   VIF   Nbr    DR    DR          BSR
CISCO    Neighbor
                                         Index   Mode   Flag  Count  Pri               Border
Neighbor Filter
10.1.4.2        register_vif0            1       v2/S   UP
10.1.4.2        gigabitethernet0         0       v2/S   UP    1      1     10.1.4.2    FALSE
FALSE
10.1.5.1        gigabitethernet1         2       v2/S   UP    0      1     10.1.5.1    FALSE
FALSE
```

```
Device4#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 1 Neighbor entry

Neighbor        Interface              Uptime/Expires    Ver   DR
Address                                                        Priority/Mode
10.1.4.1        gigabitethernet0       23:03:12/00:01:20 v2    1 /
```

**Note:**

- The viewing method of Device1, Device2, Device3 is the same as that of Device4, so the viewing process is omitted.

#View the BSR and RP information of Device4.

```
Device4#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
  BSR address: 23.23.23.23
  BSR Priority: 0
  Hash mask length: 10
  Up time: 01:57:44
  Expiry time: 00:01:28
  Role: Non-candidate BSR
  State: Accept Preferred

Device4#show ip pim rp mapping
PIM Group-to-RP Mappings Table:
PIM VRF Name: Default
Total 1 RP set entry
Total 1 RP entry

  Group(s): 224.0.0.0/4
  RP count: 1
    RP: 22.22.22.22
      Info source: 23.23.23.23, via bootstrap, priority 192
      Up time: 01:57:45
      Expiry time: 00:01:47
```

#View the BSR and RP information of Device1.

```
Device1#show ip pim bsr-router
```

```
PIMv2 Bootstrap information
PIM VRF Name: Default
  BSR address: 12.12.12.12
  BSR Priority: 0
  Hash mask length: 10
  Up time: 02:00:24
  Expiry time: 00:01:44
  Role: Non-candidate BSR
  State: Accept Preferred

Device1#show ip pim rp mapping
PIM Group-to-RP Mappings Table:
PIM VRF Name: Default
Total 1 RP set entry
Total 1 RP entry

  Group(s): 224.0.0.0/4
  RP count: 1
    RP: 11.11.11.11
      Info source: 12.12.12.12, via bootstrap, priority 192
      Up time: 02:00:30
      Expiry time: 00:01:58
```

You can see that there is only the BSR and RP information of the belonging multicast domain on Device4, Device1.

**Note:**

- The viewing method of Device2 and Device3 is the same as that of Device1, Device4, so the viewing process is omitted.

**Step 4:** Configure MP-EBGP. Set up the direct-connected EBGP peer between Device2 and Device3 and use the MBGP to interact the multicast route.

#Configure Device2.

Configure setting up the direct-connected EBGP peer with Device3, enable Multicast address stack and advertise the multicast route.

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 10.1.3.2 remote-as 200
Device2(config-bgp)#address-family ipv4 multicast
Device2(config-bgp-af)#network 10.1.1.0 255.255.255.0
Device2(config-bgp-af)#network 11.11.11.11 255.255.255.255
Device2(config-bgp-af)#neighbor 10.1.3.2 activate
```

```
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

#Configure Device3.

Configure setting up the direct-connected EBGP peer with Device2, enable Multicast address stack and advertise the multicast route.

```
Device3(config)#router bgp 200
Device3(config-bgp)#neighbor 10.1.3.1 remote-as 100
Device3(config-bgp)#address-family ipv4 multicast
Device3(config-bgp-af)#network 10.1.5.0 255.255.255.0
Device3(config-bgp-af)#network 22.22.22.22 255.255.255.255
Device3(config-bgp-af)#neighbor 10.1.3.1 activate
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#exit
```

#View the BGP neighbor status of Device3.

```
Device3#show ip bgp summary
BGP router identifier 22.22.22.22, local AS number 200
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.1.3.1        4   100     114     111        2    0    0 01:35:00        0

Total number of neighbors 1
```

According to the number displayed in the State/PfxRcd list (the number of the unicast route prefixes received from the neighbor), we can see that the BGP neighbor is set up between Device3 and Device2 successfully.

#View the BGP Multicast route table of Device3.

```
Device3#show bgp ipv4 multicast
BGP table version is 9, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
[B]*> 10.1.1.0/24     10.1.3.1                 2             0 100 i
[B]*> 10.1.5.0/24     10.1.4.2                 2         32768 i
[B]*> 11.11.11.11/32  10.1.3.1                 0             0 100 i
[B]*> 22.22.22.22/32  0.0.0.0                  0         32768 i
```

You can see that Device3 learns the Source and RP routes of the multicast domain PIM-SM1 and the next hop is MSDP peer 10.1.3.1.

**Note:**

- The viewing method of Device2 is the same as that of Device3, so the viewing process is omitted.

**Step 5:** Configure MSDP.

#Configure Device2.

Configure setting up the direct-connected EBGP peer with Device3; enable the function of actively sending the SA request packet to the specified peer; configure using the RFC3618 rule to perform the RPF check for the MSDP packet.

```
Device2(config)#ip msdp peer 10.1.3.2 remote-as 200
Device2(config)#ip msdp sa-request 10.1.3.2
Device2(config)#ip msdp rpf rfc3618
```

#Configure Device3.

Configure setting up the direct-connected EBGP peer with Device2; enable the function of actively sending the SA request packet to the specified peer; configure using the RFC3618 rule to perform the RPF check for the MSDP packet.

```
Device3(config)#ip msdp peer 10.1.3.1 remote-as 100
Device3(config)#ip msdp sa-request 10.1.3.1
Device3(config)#ip msdp rpf rfc3618
```

#View the MSDP peer connection status and details of Device3.

```
Device3#show ip msdp summary
MSDP Peer Status Summary
Total 1 Peer entry
Peer Address    AS    State    Reset  Uptime/Downtime
10.1.3.1        100   Up       0      02:21:18

Device3#show ip msdp peer
MSDP Peer Table:
Total 1 Peer entry
MSDP Peer 10.1.3.1, AS 100 (configured AS)
  Connection status:
    State: Established, Resets: 0, Connection source: none configured
    Uptime(Downtime): 02:50:00, Message sent/received: 136/161
    Connection and counters cleared 02:13:25 ago
    Local Address of connection: 10.1.3.2
    Remote Address of connection: 10.1.3.1
    Local Port: 639, Remote Port: 1179
```

```
SA-Requests:
  Input filter: none
  Sending SA-Requests to peer: enabled
SA:
  Input filter: none
Message counters:
  RPF Failure count: 0
  SA Messages in/out: 47/0
  SA Requests in/out: 0/3
  SA Responses in/out: 3/0
Data Packets in/out: 0/0
```

You can see that the MSDP peer connection is set up successfully between Device3 and Device2.

**Note:**

- The viewing method of Device2 is the same as that of Device3, so the viewing process is omitted.

**Step 6:** Check the result.

#Receiver sends the IGMPv2 member report packet to add to multicast group 225.1.1.1; Source sends the multicast service packet with multicast group 225.1.1.1.

#View the multicast member table on Device4.

```
Device4#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address   Interface          Uptime   Expires  Last Reporter  V1 Expires
225.1.1.1       gigabitethernet1   00:05:11 00:02:38 10.1.5.2       stopped
```

#View the MSDP SA cache information of Device2.

```
Device2#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(10.1.1.2, 225.1.1.1), RP 11.11.11.11, Originated, 00:11:45/00:05:39
```

You can see that Device2 generates and caches the SA packet. The multicast source address in the SA packet is 10.1.1.2; the multicast group address is 225.1.1.1; the RP address is 11.11.11.11.

#View the MSDP SA cache information and RPF check table of Device3.

```
Device3#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(10.1.1.2, 225.1.1.1), RP 11.11.11.11, Recv From Peer 10.1.3.1, 00:08:39/00:05:21

Device3#show ip msdp rpf
```

```
Destination     Nexthop        Nexthop         Nexthop Metric  Pref    -
Address         Address        From            RefCnt
10.1.3.1        0.0.0.0        0.0.0.0         1       10      0
11.11.11.11     10.1.3.1       10.1.3.1        1       0       20
```

You can see that Device3 receives and caches the SA packet. The SA packet is from the peer 10.1.3.1. The multicast source address in the packet is 10.1.1.2; the multicast group address is 225.1.1.1; the RP address is 11.11.11.11; the next hop of on the best path from Device3 to source end RP (11.11.11.11) is 10.1.3.1.

#View the PIM-SM multicast route table of Device3.

```
Device3#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(*, 225.1.1.1)
Up time: 00:13:57
RP: 22.22.22.22
RPF nbr: 0.0.0.0
RPF idx: None
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    gigabitethernet1  00:13:57/00:02:33
  Asserted interface list:


(10.1.1.2, 225.1.1.1)
Up time: 00:13:57
KAT time: 00:03:28
RPF nbr: 10.1.3.1
```

```
RPF idx: gigabitethernet0
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 6906038

(10.1.1.2, 225.1.1.1, rpt)
Up time: 00:13:57
RP: 22.22.22.22
Flags:
  RPT JOIN DESIRED
  PRUNE DESIRED
  RPF SGRPT XG EQUAL
Upstream State: PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    gigabitethernet1
```

#Receiver can receive the multicast service packet with multicast group 225.1.1.1 sent by Source.

**Note:**

- The viewing method of Device2 is the same as that of Device3, so the viewing process is omitted.

## 9.3.2. Configure Anycast RP

### Network Requirements

- The whole PIM multicast domain runs the PIM-SM protocol.
- Loopback0 interface of Device3 is C-BSR. Loopback1 interfaces of Device2 and Device4 are C-RP and the IP addresses are the same.
- Use the IP address of Loopback0 between Device2 and Device4 to set up the MSDP peer connection.
- In the domain, configure multiple RPs with the same address; non-RP device selects the nearest RP used to manage the multicast source and receiver. The RPs exchange the multicast source information via MSDP so that the multicast service of the whole

multicast domain can be interacted. If one RP fails, its managed areas are shared by other RPs.

## Network Topology

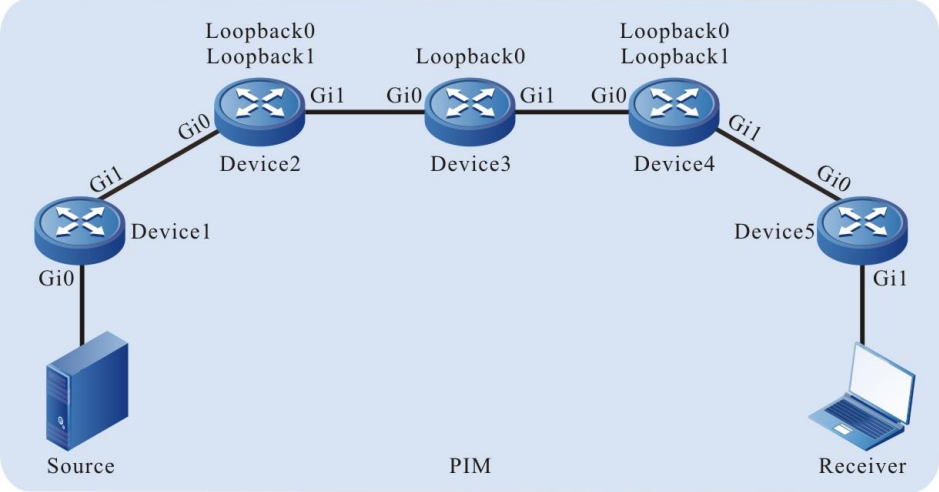


Figure 9-2 Networking of configuring Anycast RP

| Device | Interface | IP address | Device | Interface | IP address |
|---|---|---|---|---|---|
| Device1 | Gi0 | 10.1.1.1/24 | Device3 | Loopback0 | 44.44.44.44/32 |
| | Gi1 | 10.1.2.1/24 | Device4 | Gi0 | 10.1.4.2/24 |
| Device2 | Gi0 | 10.1.2.2/24 | | Gi1 | 10.1.5.1/24 |
| | Gi1 | 10.1.3.1/24 | | Loopback0 | 22.22.22.22/32 |
| | Loopback0 | 11.11.11.11/32 | | Loopback1 | 55.55.55.55/32 |
| | Loopback1 | 55.55.55.55/32 | Device5 | Gi0 | 10.1.5.2/24 |
| Device3 | Gi0 | 10.1.3.2/24 | | Gi1 | 10.1.6.1/24 |
| | Gi1 | 10.1.4.1/24 | Source | - | 10.1.1.2/24 |

## Configuration Steps

**Step 1:** Configure the IP address of the interface. (omitted)

**Step 2:** Configure OSPF so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
```

```
Device1(config)#router ospf 100
Device1(config-ospf)#network 10.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.1.2.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device2(config-ospf)#network 11.11.11.11 0.0.0.0 area 0
Device2(config-ospf)#network 55.55.55.55 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 10.1.3.0 0.0.0.255 area 0
Device3(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
Device3(config-ospf)#network 44.44.44.44 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#Configure Device4.

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#network 10.1.4.0 0.0.0.255 area 0
Device4(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
Device4(config-ospf)#network 22.22.22.22 0.0.0.0 area 0
Device4(config-ospf)#network 55.55.55.55 0.0.0.0 area 0
Device4(config-ospf)#exit
```

#Configure Device5.

```
Device5#configure terminal
Device5(config)#router ospf 100
Device5(config-ospf)#network 10.1.5.0 0.0.0.255 area 0
Device5(config-ospf)#network 10.1.6.0 0.0.0.255 area 0
Device5(config-ospf)#exit
```

#View the route table of Device5.

```
Device5#show ip route
Codes: C - connected, S - static, R - RIP,  O - OSPF, OE-OSPF External, M - Management
```

```
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   10.1.1.0/24 [110/5] via 10.1.5.1, 04:04:37, gigabitethernet0
O   10.1.2.0/24 [110/4] via 10.1.5.1, 04:05:13, gigabitethernet0
O   10.1.3.0/24 [110/3] via 10.1.5.1, 04:17:36, gigabitethernet0
O   10.1.4.0/24 [110/2] via 10.1.5.1, 18:19:08, gigabitethernet0
C   10.1.5.0/24 is directly connected, 18:22:13, gigabitethernet0
C   10.1.6.0/24 is directly connected, 04:32:51, gigabitethernet1
O   11.11.11.11/32 [110/4] via 10.1.5.1, 04:17:36, gigabitethernet0
O   22.22.22.22/32 [110/2] via 10.1.5.1, 03:56:25, gigabitethernet0
O   44.44.44.44/32 [110/3] via 10.1.5.1, 04:13:23, gigabitethernet0
O   55.55.55.55/32 [110/2] via 10.1.5.1, 04:17:36, gigabitethernet0
```

#We can see that Device5 leans the routes of multicast source, BSR and RP.

**Note:**

- The viewing method of Device1, Device2, Device3, and Device4 is the same as that of Device5, so the viewing process is omitted.

**Step 4:** Globally enable the multicast forwarding, enable the multicast protocol PIM-SM on the interface, and configure C-BSR and C-RP.

#Configure Device1.

Globally enable the multicast forwarding, and enable the multicast protocol PIM-SM on the interface.

```
Device1(config)#ip multicast-routing
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip pim sparse-mode
Device1(config-if-gigabitethernet0)#exit
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#ip pim sparse-mode
Device1(config-if-gigabitethernet1)#exit
```

#Configure Device2.

Globally enable the multicast forwarding, enable the multicast protocol PIM-SM on the interface, and configure Loopback1 as C-RP; the multicast group range of the C-RP service is 224.0.0.0/4.

```
Device2(config)#ip multicast-routing
Device2(config)#interface loopback0
Device2(config-if-loopback0)#ip pim sparse-mode
```

```
Device2(config-if-loopback0)#exit
Device2(config)#interface loopback1
Device2(config-if-loopback1)#ip pim sparse-mode
Device2(config-if-loopback1)#exit
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ip pim sparse-mode
Device2(config-if-gigabitethernet0)#exit
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#ip pim sparse-mode
Device2(config-if-gigabitethernet1)#exit
Device2(config)#ip pim rp-candidate loopback1
```

#Configure Device3.

Globally enable the multicast forwarding, enable the multicast protocol PIM-SM on the interface, and configure Loopback0 as C-BSR.

```
Device3(config)#ip multicast-routing
Device3(config)#interface loopback0
Device3(config-if-loopback0)#ip pim sparse-mode
Device3(config-if-loopback0)#exit
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#ip pim sparse-mode
Device3(config-if-gigabitethernet0)#exit
Device3(config)#interface gigabitethernet1
Device3(config-if-gigabitethernet1)#ip pim sparse-mode
Device3(config-if-gigabitethernet1)#exit
Device3(config)#ip pim bsr-candidate loopback0
```

#Configure Device4.

Globally enable the multicast forwarding, enable the multicast protocol PIM-SM on the interface, and configure Loopback1 as C-RP; the multicast group range of the C-RP service is 224.0.0.0/4.

```
Device4(config)#ip multicast-routing
Device4(config)#interface loopback0
Device4(config-if-loopback0)#ip pim sparse-mode
Device4(config-if-loopback0)#exit
Device4(config)#interface loopback1
Device4(config-if-loopback1)#ip pim sparse-mode
Device4(config-if-loopback1)#exit
Device4(config)#interface gigabitethernet0
Device4(config-if-gigabitethernet0)#ip pim sparse-mode
```

```
Device4(config-if-gigabitethernet0)#exit
Device4(config)#interface gigabitethernet1
Device4(config-if-gigabitethernet1)#ip pim sparse-mode
Device4(config-if-gigabitethernet1)#exit
Device4(config)#ip pim rp-candidate loopback1
```

#Configure Device5. Globally enable the multicast forwarding and enable the multicast protocol PIM-SM on the interface.

```
Device5(config)#ip multicast-routing
Device5(config)#interface gigabitethernet0
Device5(config-if-gigabitethernet0)#ip pim sparse-mode
Device5(config-if-gigabitethernet0)#exit
Device5(config)#interface gigabitethernet1
Device5(config-if-gigabitethernet1)#ip pim sparse-mode
Device5(config-if-gigabitethernet1)#exit
```

#View the information of the interface enabled with the PIM-SM protocol on Device5 and the PIM-SM neighbor information.

```
Device5#show ip pim interface
PIM Interface Table:
PIM VRF Name: Default
Total 3 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Address         Interface                VIF     Ver/  VIF   Nbr    DR    DR          BSR
CISCO    Neighbor
                                         Index    Mode   Flag  Count  Pri               Border
Neighbor Filter
10.1.5.2        register_vif0            1       v2/S   UP
10.1.5.2        gigabitethernet0         0       v2/S   UP    1      1     10.1.5.2    FALSE
FALSE
10.1.6.1        gigabitethernet1         2       v2/S   UP    0      1     10.1.6.1    FALSE
FALSE

Device5#show ip pim neighbor
PIM Neighbor Table:
PIM VRF Name: Default
Total 1 Neighbor entry
```

```
Neighbor        Interface               Uptime/Expires    Ver   DR
Address                                                         Priority/Mode
10.1.5.1        gigabitethernet0        18:37:22/00:01:45 v2    1 /
```

#View the BSR and RP information of Device5.

```
Device5#show ip pim bsr-router
PIMv2 Bootstrap information
PIM VRF Name: Default
  BSR address: 44.44.44.44
  BSR Priority: 0
  Hash mask length: 10
  Up time: 04:36:44
  Expiry time: 00:01:35
  Role: Non-candidate BSR
  State: Accept Preferred
Device5#show ip pim rp mapping
PIM Group-to-RP Mappings Table:
PIM VRF Name: Default
Total 1 RP set entry
Total 1 RP entry

  Group(s): 224.0.0.0/4
  RP count: 1
    RP: 55.55.55.55
      Info source: 44.44.44.44, via bootstrap, priority 192
      Up time: 04:36:44
      Expiry time: 00:01:53
```

**Note:**

- The viewing method of Device1, Device2, Device3, Device4 is the same as that of Device5, so the viewing process is omitted.

**Step 4:** Configure MSDP.

#Configure Device2.

Configure setting up the non-direct-connected MSDP peer connection via Loopback0 with Loopback0 of Device4; enable the function of actively sending the SA request packet to the specified peer; configure the RP address in the SA packet as the IP address of Loopback0; configure using the RFC3618 rule to perform the RPF check for the MSDP packet.

```
Device2(config)#ip msdp peer 22.22.22.22 connect-source loopback0
```

```
Device2(config)#ip msdp sa-request 22.22.22.22
Device2(config)#ip msdp originator-id loopback0
Device2(config)#ip msdp rpf rfc3618
```

#Configure Device4.

Configure setting up the non-direct-connected MSDP peer connection via Loopback0 with Loopback0 of Device2; enable the function of actively sending the SA request packet to the specified peer; configure the RP address in the SA packet as the IP address of Loopback0; configure using the RFC3618 rule to perform the RPF check for the MSDP packet.

```
Device4(config)#ip msdp peer 11.11.11.11 connect-source loopback0
Device4(config)#ip msdp sa-request 11.11.11.11
Device4(config)#ip msdp originator-id loopback0
Device4(config)#ip msdp rpf rfc3618
```

#View the MSDP peer connection status and details of Device4.

```
Device4#show ip msdp summary
MSDP Peer Status Summary
Total 1 Peer entry
Peer Address     AS     State    Reset  Uptime/Downtime
11.11.11.11      ?      Up       0      05:49:35

Device4#show ip msdp peer
MSDP Peer Table:
Total 1 Peer entry
MSDP Peer 11.11.11.11, AS ?
  Connection status:
    State: Established, Resets: 0, Connection source: loopback0
    Uptime(Downtime): 05:49:39, Message sent/received: 352/528
    Connection and counters cleared 05:53:24 ago
    Local Address of connection: 22.22.22.22
    Remote Address of connection: 11.11.11.11
    Local Port: 639, Remote Port: 1053
  SA-Requests:
    Input filter: none
    Sending SA-Requests to peer: enabled
  SA:
    Input filter: none
  Message counters:
    RPF Failure count: 3
    SA Messages in/out: 348/0
```

```
    SA Requests in/out: 0/3
    SA Responses in/out: 2/0
  Data Packets in/out: 0/0
```

You can see that Device4 and Device2 set up the MSDP peer connection successfully.

**Note:**

- The viewing method of Device2 is the same as that of Device4, so the viewing process is omitted.

**Step 5:** Check the result.

# Source sends the multicast service packet with multicast group 225.1.1.1.

#View the MSDP SA cache information of Device2.

```
Device2#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(10.1.1.2, 225.1.1.1), RP 55.55.55.55, Originated, 00:03:34/00:05:43
```

You can see that Device2 generates and caches the SA packet. The multicast source address in the SA packet is 10.1.1.2; the multicast group address is 225.1.1.1; the RP address is 55.55.55.55.

#View the MSDP SA cache information and RPF check table of Device4.

```
Device4#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
(10.1.1.2, 225.1.1.1), RP 11.11.11.11, Recv From Peer 11.11.11.11, 00:07:02/00:05:58

Device4#show ip msdp rpf
Destination     Nexthop        Nexthop         Nexthop Metric  Pref
Address         Address        From            RefCnt
10.1.4.1        0.0.0.0        0.0.0.0         1       10      0
11.11.11.11     10.1.4.1       55.55.55.55     3       3       110
55.55.55.55     0.0.0.0        0.0.0.0         2       1       0
```

You can see that Device4 receives and caches the SA packet. The SA packet is from the peer 11.11.11.11. The multicast source address in the packet is 10.1.1.2; the multicast group address is 225.1.1.1; the RP address is 11.11.11.11.

**Note:**

- If **ip msdp originator-id** is configured on the source RP and when it sends the SA packet to MSDP peer, it replaces the RP address in the packet with the IP address of the specified interface.

#View the PIM-SM multicast route table of Device2.

```
Device2#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
```

```
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(10.1.1.2, 225.1.1.1)
Up time: 00:01:14
KAT time: 00:03:23
RPF nbr: 10.1.2.1
RPF idx: gigabitethernet0
SPT bit: FALSE
Flags:
Upstream State: NOT JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
  Packet count 0

(10.1.1.2, 225.1.1.1, rpt)
Up time: 00:01:14
RP: 55.55.55.55
Flags:
  RPF SGRPT XG EQUAL
Upstream State: RPT NOT JOINED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
```

#View the PIM-SM multicast route table of Device4.

```
Device4#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
```

```
Total 0 (S,G) entry
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer
```

You can see that there is (10.1.1.2, 225.1.1.1) entry on Device2 and no (10.1.1.2, 225.1.1.1) entry on Device4. It indicates that Source initiates the PIM-SM register to the nearest RP, that is, Device2.

#Receiver sends the IGMPv2 member report packet to add to multicast group 225.1.1.1.

#View the multicast member table on Device5.

```
Device5#show ip igmp groups
IGMP Connected Group Membership
Total 1 groups
Group Address   Interface            Uptime   Expires  Last Reporter   V1 Expires
225.1.1.1       gigabitethernet1     00:00:12 00:04:12 10.1.6.2        stopped
```

#View the PIM-SM multicast route table of Device2.

```
Device2#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(10.1.1.2, 225.1.1.1)
Up time: 00:19:01
KAT time: 00:03:14
RPF nbr: 10.1.2.1
RPF idx: gigabitethernet0
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
```

```
  Joined interface list:
    gigabitethernet1  00:02:56/00:02:34
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 1136269

(10.1.1.2, 225.1.1.1, rpt)
Up time: 00:19:01
RP: 55.55.55.55
Flags:
  RPF SGRPT XG EQUAL
Upstream State: RPT NOT JOINED
```

#View the PIM-SM multicast route table of Device4.

```
Device4#show ip pim mroute
IP Multicast Routing Table:
PIM VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(*, 225.1.1.1)
Up time: 00:05:54
RP: 55.55.55.55
RPF nbr: 0.0.0.0
RPF idx: None
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    gigabitethernet1  00:05:54/00:02:36
  Asserted interface list:
```

```
(10.1.1.2, 225.1.1.1)
Up time: 00:05:54
KAT time: 00:03:22
RPF nbr: 10.1.4.1
RPF idx: gigabitethernet0
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
    gigabitethernet1  00:05:54/00:02:37
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet1
  Packet count 2172581

(10.1.1.2, 225.1.1.1, rpt)
Up time: 00:05:54
RP: 55.55.55.55
Flags:
  RPT JOIN DESIRED
  PRUNE DESIRED
  RPF SGRPT XG EQUAL
Upstream State: PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    gigabitethernet1
```

You can see that there is (*,225.1.1.1) entry on Device4 and no (*,225.1.1.1) entry on Device2. It indicates that Source initiates the PIM-SM adding to the nearest RP, that is, Device4.

#Receiver can receive the multicast service packet with multicast group 225.1.1.1 sent by Source.

# 10. MLD

## 10.1. Overview

MLD is short for Multicast Listener Discovery Protocol, used to set up and maintain the multicast group member relation between the IPv6 host and its dirst neighboring multicast device.

MLD router uses the local address of the IPv6 unicast link as the source address to send the MLD packet. MLD uses ICMPv6 (Internet Control Message Protocol for IPv6) packet type. All MLD packets are limited on the local link, and the hops are 1.

MLD has two versions: MLDv1n corresponds to IGMPv2, and MLDv2 corresponds to IGMPv3.

The packet types of the IGMP protocol adopting the IP protocol number 2 are different. The MLD protocol adopts the ICMPv6 (IP protocol number is 58) packet type, including MLD query packet (type value is 130), MLDv1 report packet (type value is 131), MLDv1 leave packet (type value is 132), and MLDv2 report packet (type value is 143). The MLD protocol and IGMP protocol have different packet formats, but have the same protocol actions.

## 10.2. MLD Function Configuration

Table 10-1 MLD function configuration list

| Configuration tasks | |
|---|---|
| Configure the MLD basic functions | Enable the MLD protocol in the interface |
| Adjust and optimize the MLD network | Configure the query interval of the general group |
| | Configure the robustness factor |
| | Configure the maximum response time |
| | Configure the specified group query |
| | Configure the fast leave |
| Configure the MLD SSM mapping | Configure the MLD SSM mapping |

### 10.2.1. Configure MLD Basic Functions

#### Configuration Condition

Before configuring the MLD basic functions, first complete the following task:

- Enable the interface IPv6
- Enable the interface MLD

### Enable the MLD Protocol

Table 10-2 Enable the MLD protocol

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable the IPv6 multicast forwarding | **ipv6 multicast-routing** [ **vrf** *vrf-name* ] | Mandatory<br>By default, the IPv6 multicast forwarding is disabled. |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Enable the MLD protocol | **ipv6 mld enable** | Mandatory<br>By default, do not enable MLD.<br>After enabling MLD, all MLD configurations can take effect. |

### Configure the MLD Version

Table 10-3 Configure the MLD version

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Configure the MLD version | **ipv6 mld version** *version-number* | Mandatory<br>By default, the MLD version is 2. |

**Caution:**

- Because the packet structure and kind of different versions of MLD protocols are different, it is suggested to configure the same version of IGMP for all devices on the same subnet.

### Configure Static Group Adding

After configuring one static group or source group in the interface, the device regards that the interface has the receiver of the multicast group or source group.

Table 10-4 Configure static group adding

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Configure the static group adding | **ipv6 mld static-group** *group-ipv6-address* [ *source-ipv6-address* ] | Mandatory<br>By default, the interface is not added to any multicast group or source group in the static mode. |

### Configure Multicast Group Filter

The interface configured with the MLD multicast group filter filters the group member relation report in the segment according to the ACL rules and only the group member relation report permitted by ACL is processed and the un-permitted is directly dropped. For the existing but not permitted by ACL multicast group, immediately delete the multicast group information.

Table 10-5 Configure multicast group filter

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Configure the IGMP multicast group filter | **ipv6 mld access-group** { *access-list-number* \| *access-list-name* } | Mandatory<br>By default, the multicast group filter is not configured. |

**Note:**

- The **ipv6 mld access-group** command only supports the standard ACL.

## 10.2.2. Adjust and Optimize the MLD Network

### Configuration Condition

Before adjusting and optimizing the MLD network, first complete the following tasks:

- Enable the IPv6 protocol
- Enable the MLD protocol on the interface

### Configure Query Interval of General Group

MLD querier periodically sends the general group query packets to maintain the group member relation. You can modify the interval of sending the MLD general group query packets according to the actuality of the network.

Table 10-6 Configure the query interval of the general group

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Configure the query interval of the general group | **ipv6 mld query-interval** *interval-value* | Optional<br>By default, the interval of sending the MLD general group query packets is 125s. |

**Note:**

- The genera query intervals of the devices on the same segment should try to keep consistent.
- The general group query interval should be larger than the maximum response time. Otherwise, the configuration cannot succeed.

### Configure Robustness Factor

The robustness factor is used to prevent the packet loss.

Table 10-7 Configure the robustness factor

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Configure the robustness factor | **ipv6 mld robustness-variable** *variable-value* | Optional<br>By default, the robustness factor of the MLD querier is 2. |

**Note:**

- After configuring the robustness factor, the following parameters also change with the robustness parameters:

1. Group member timeout = Robustness factor * general group query time + maximum response time;
2. Other querier timeout = Robustness factor * general group query time + maximum response time/2;
3. The larger the robustness factor, the larger the MLD group member timeout and other querier timeout. Set the value according to the actuality of the network.

### Configure Maximum Response Time

The general group query packet sent by the querier contains the maximum response time field and the receiver sends the group member relation report within the maximum response interval. If the receiver does not send the group member relation report within the maximum response time, the device regards that the subnet does not have the receiver of the multicast group and deletes the multicast group information immediately.

Table 10-8 Configure the maximum response time

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Configure the maximum response time | **ipv6 mld query-max-response-time** *seconds* | Optional<br>By default, the maximum response time of the MLD general group query is 10s. |

### Configure Specified Group Query

After the MLD querier receives the leave packet of one multicast group, send the specified group query packet to query the multicast group on the segment. The sending times of the packet depends on “Specified group query times”. This is to know whether the subnet has the members of the multicast group. If not receiving the member relation report of the multicast group after waiting for “maximum response time”, delete the information of the multicast group.

Table 10-9 Configure the specified group query

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Configure the query interval of the specified group | **ipv6 mld last-member-query-interval** *interval-value* | Optional<br>By default, the interval of sending the specified group query packets is 1s. |
| Configure the query times of the specified group | **ipv6 mld last-member-query-count** *count-value* | Optional<br>By default, the times of sending the specified group query packets is 2. |

### Configure Fast Leave

The end segment in the network only connects to one host, which performs the switching action of the multicast group frequently. To reduce the leave delay, you can configure the fast leave of the multicast group on the device.

After configuring the fast leave, the device receives the leave packet of one multicast group and checks whether the multicast group belongs to the fast leave range. If yes, the device does not send the specified group query packet to the segment any more and deletes the information of the multicast group immediately.

Table 10-10 Configure the fast leave

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Configure the source group range of the fast leave | **ipv6 mld immediate-leave group-list** { *access-list-number* \| *access-list-name* } | Mandatory<br>By default, do not permit the fast leave of the multicast group |

## 10.2.3. Configure the MLD SSM Mapping

### Configuration Condition

Before configuring the MLD SSM mapping, first complete the following tasks:

- Enable the interface IPv6
- Enable the interface MLD

### Configure the MLD SSM Mapping

To provide the PIM-SMv6 SSM service for the receiver not supporting MLDv2 in the PIM-SMv6 SSM network, we can configure the MLD SSM Mapping function on the device.

The user can configure the MLD SSM Mapping rule according to the demand of the network receiver. The group member relation report permitted by the rule is converted to the MLD non-member (IS_EX, TO_EX) relation report, and the multicast source address is the source address specified by the MLD SSM mapping rule.

Table 10-11 Configure the MLD SSM mapping

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable MLD SSM Mapping | **ipv6 mld ssm-map enable** [ **vrf** *vrf-name* ] | Mandatory<br>By default, MLD SSM Mapping is not enabled. |
| Configure the MLD SSM Mapping rule | **ipv6 mld ssm-map static** { *access-list-number* **\|** *access-list-name* } *source-ipv6-address* [ **vrf** *vrf-name* ] | Mandatory<br>By default, there is no MLD SSM Mapping rule. |

**Note:**

- The **ipv6 mld ssm-map** static command only supports the extended ACL.

### 10.2.4. MLD Monitoring and Maintaining

Table 10-12 MLD monitoring and maintaining

| Command | Description |
|---|---|
| **clear ipv6 mld group** [ *group-ipv6-address* ] [ *interface-name* ] [ **vrf** *vrf-name* ] | Clear the MLD multicast group information |
| **clear ipv6 mld statistic interface** *interface-name* | Clear the MLD packet statistics information on the interface |
| **show ipv6 mld groups** [ [ **static** ] \| [ *interface-name* ] [ *group-ipv6-address* ] [ **detail** ] ] [ **vrf** *vrf-name* ] | Display the MLD multicast group information |
| **show ipv6 mld interface** [ *interface-name* ] [ **vrf** *vrf-name* ] | Display the interface MLD information |
| **show ipv6 mld statistic interface** *interface-name* [ **vrf** *vrf-name* ] | Display the statistics information of the MLD packets |

## 10.3. MLD Typical Configuration Example

### 10.3.1. Configure MLD Basic Functions

#### Network Requirements

- The whole network runs the PIM-SMv6 protocol.
- Device1, Device2, and Receiver are in the same LAN and Device1 is the querier.
- Receiver is one receiver of Device1 and Device2 stub network.
- Run MLDv2 between Device1, Device2 and stub network.

#### Network Topology

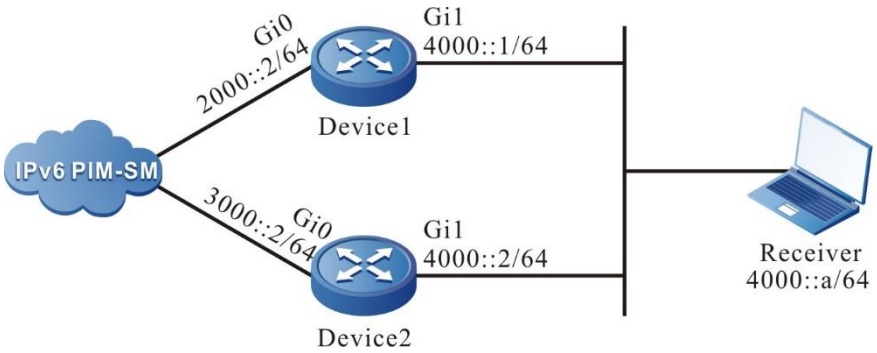


Figure 10-1 Networking of configuring MLD basic functions

#### Configuration Steps

**Step 1:** Configure the IPv6 address of the interface (omitted).

**Step 2:** Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the interface. Enable MLD on the interface of Device1 and Device2 connecting the Receiver.

#Configure Device1.

Globally enable the IPv6 multicast forwarding, enable the multicast protocol PIM-SMv6 on the related interfaces, and enable MLD on the interface of connecting Receiver.

```
Device1#configure terminal
Device1(config)#ipv6 multicast-routing
Device1(config)#interface gigabitethernet0/0/0
Device1(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/0)#exit
Device1(config)#interface gigabitethernet0/0/1
Device1(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/1)#ipv6 mld enable
Device1(config-if-gigabitethernet0/0/1)#exit
```

#Configure Device2.

Globally enable the IPv6 multicast forwarding, enable the multicast protocol PIM-SMv6 on the related interfaces, and enable MLD on the interface of connecting Receiver.

```
Device2#configure terminal
```

```
Device2(config)#ipv6 multicast-routing
Device2(config)#interface gigabitethernet0/0/0
Device2(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device2(config-if-gigabitethernet0/0/0)#exit
Device2(config)#interface gigabitethernet0/0/1
Device2(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device2(config-if-gigabitethernet0/0/1)#ipv6 mld enable
Device2(config-if-gigabitethernet0/0/1)#exit
```

**Step 3:** Check the result.

#View the MLD version information and querier election result of Device1 interface gigabitethernet0/0/1.

```
Device1#show ipv6 mld interface gigabitethernet 1
Interface gigabitethernet0/0/1 (Index 23)
 MLD Enabled, Active
 Querier: fe80::201:2ff:fe03:406 (Self)
 Default version: 2
 Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  Query response time is 10 seconds
          Last member query response interval is 1 seconds
          Last member query count is 2
          Group Membership interval is 260 seconds
  Robustness variable is 2
```

#View the MLD version information and querier election result of Device2 interface gigabitethernet0/0/1.

```
Device2#show ipv6 mld interface gigabitethernet 1
Interface gigabitethernet0/0/1 (Index 50331674)
 MLD Enabled, Active
 Querier: fe80::201:2ff:fe03:406
 Non-Querier: fe80::201:7aff:febc:662b Expires: 00:04:07
 Default version: 2
 Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  Query response time is 10 seconds
  Last member query response interval is 1 seconds
```

```
Last member query count is 2
Group Membership interval is 260 seconds
Robustness variable is 2
```

# Receiver sends the MLDv2 member report packet to add to multicast group FF1E::1.

#View the multicast member table of Device1.

```
Device1#show ipv6 mld groups
MLD Connected Group Membership
Total 1 Connected Groups
Group        Interface        Uptime    Expires  V1-Expires Last Reporter
ff1e::1      gigabitethernet0/0/1  00:00:02  00:04:17 not used   fe80::b
```

#View the multicast member table of Device2.

```
Device2#show ipv6 mld groups
MLD Connected Group Membership
Total 1 Connected Groups
Group        Interface        Uptime    Expires  V1-Expires Last Reporter
ff1e::1      gigabitethernet0/0/1  00:00:02  00:04:17 not used   fe80::b
```

**Note:**

- On the interface, run the MLDv2 version, be compatible with the MLDv1 member relation report and MLDv1 member leave packet by default. You can configure the running MLD version of the interface via the command ipv6 mld version.
- When multiple devices run MLD in one LAN, elect the MLD querier and the one with the smallest address is elected as the MLD querier of the LAN.

## 10.3.2. Configure IGMP Static Adding

### Network Requirements

- The whole network runs the PIM-SMv6 protocol.
- Receiver is one receiver of the Device stub network.
- Run MLDv2 between Device and the stub network.
- Device interface gigabitethernet0/0/1 adds to multicast group FF1E::1 statically.

### Network Topology

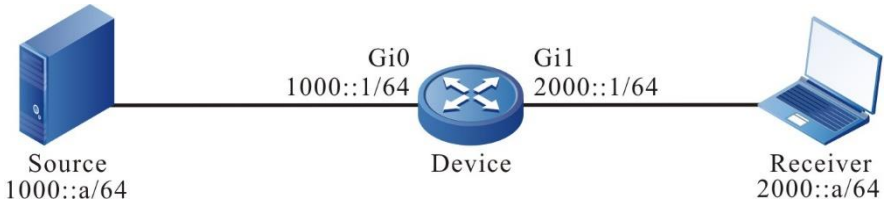


Figure 10-2 Networking of configuring MLD static adding

### Configuration Steps

**Step 1:** Configure the IPv6 address of the interface (omitted).

**Step 2:** Globally enable the IPv6 multicast forwarding, enable the multicast protocol PIM-SMv6 on the interface. Enable MLD on the interface of connecting the Receiver.

#Configure Device.

Globally enable the IPv6 multicast forwarding, enable the multicast protocol PIM-SMv6 on the related interfaces, and enable MLD on the interface of connecting Receiver.

```
Device#configure terminal
Device(config)#ipv6 multicast-routing
Device(config)#interface gigabitethernet0/0/0
Device(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device(config-if-gigabitethernet0/0/0)#exit
Device(config)#interface gigabitethernet0/0/1
Device(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device(config-if-gigabitethernet0/0/1)#ipv6 mld enable
Device(config-if-gigabitethernet0/0/1)#exit
```

#View the MLD information of Device interface gigabitethernet0/0/1.

```
Device#show ipv6 mld interface gigabitethernet 1
Interface gigabitethernet0/0/1 (Index 23)
 MLD Enabled, Active
 Querier: fe80::201:2ff:fe03:406 (Self)
 Default version: 2
 Querier parameter:
   Query interval is 125 seconds
   Querier timeout is 255 seconds
   Query response time is 10 seconds
   Last member query response interval is 1 seconds
   Last member query count is 2
   Group Membership interval is 260 seconds
   Robustness variable is 2
```

**Step 3:** Device interface gigabitethernet 1 adds to multicast group FF1E::1 statically.

#Configure Device.

Device interface gigabitethernet 1 adds to multicast group FF1E::1 statically.

```
Device(config)#interface gigabitethernet0/0/1
Device(config-if-gigabitethernet0/0/1)#ipv6 mld static-group ff1e::1
Device(config-if-gigabitethernet0/0/1)#exit
```

**Step 4:** Check the result.

#Source sends the multicast packet with multicast group FF1E::1.

#View the multicast member table of Device.

```
Device#show ipv6 mld groups
MLD Static Group Membership
Total 1 Static Groups
Group          Source         Interface
ff1e::1        ::             gigabitethernet0/0/1
```

#View the multicast route table of Device.

```
Device#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 1 (S,G) entry
Total 1 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(*, ff1e::1)
Up time: 00:01:06
RP: ::
RPF nbr: ::
RPF idx: None
Flags:
Upstream State: NOT JOINED
Local interface list:
gigabitethernet0/0/1
Joined interface list:
Asserted interface list:

(1000::a, ff1e::1)
Up time: 00:00:04
KAT time: 00:03:26
RPF nbr: ::
```

RPF idx: None
SPT bit: TRUE
Flags:
JOIN DESIRED
COULD REGISTER
Upstream State: JOINED
Local interface list:
Joined interface list:
register_vif0
Asserted interface list:
Outgoing interface list:
register_vif0
gigabitethernet0/0/1
Packet count 1

(1000::a, ff1e::1, rpt)
Up time: 00:00:04
RP: ::
Flags:
RPT JOIN DESIRED
RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
Local interface list:
Pruned interface list:
Outgoing interface list:

#Receiver can receive the multicast packet with multicast group FF1E::1 sent by Source.

### 10.3.3. Configure MLD SSM Mapping

#### Network Requirements

- The whole network runs the PIM-SMv6 SSM protocol.
- Receiver1, Receiver2, and Device2 are all in one LAN.
- Run MLDv2 between Device2 and the stub network.
- Use the MLD SSM mapping on Device2 so that Receiver2 can only receive the multicast service packets sent by Source1.

## Network Topology

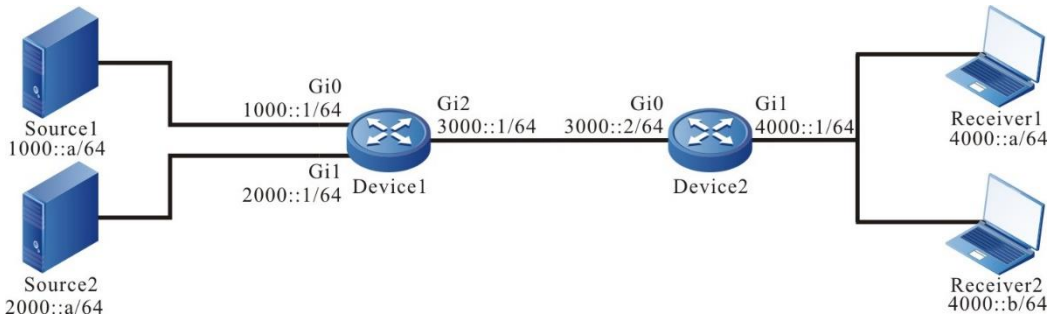


Figure 10-3 Networking of configuring the MLD SSM mapping

## Configuration Steps

**Step 1:** Configure the IPv6 address of the interface (omitted).

**Step 2:** Enable the IPv6 unicast routing OSPFv3 so that all network devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface gigabitethernet0/0/0
Device1(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/0)#exit
Device1(config)#interface gigabitethernet0/0/1
Device1(config-if-gigabitethernet0/0/1)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/1)#exit
Device1(config)#interface gigabitethernet0/0/2
Device1(config-if-gigabitethernet0/0/2)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/2)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface gigabitethernet0/0/0
Device2(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
Device2(config-if-gigabitethernet0/0/0)#exit
```

#View the route table of Device2.

```
Device2#show ipv6 route
```

```
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route O - OSPF, OE-OSPF External, M - Management

L   ::1/128 [0/0]
    via ::, 05:20:37, lo0
        O   1000::/64 [110/2]
            via fe80::201:2ff:fe03:406, 00:35:30, gigabitethernet0/0/0
O   2000::/64 [110/2]
    via fe80::201:2ff:fe03:406, 00:37:15, gigabitethernet0/0/0
C   3000::/64 [0/0]
    via ::, 00:38:24, gigabitethernet0/0/0
L   3000::2/128 [0/0]
    via ::, 00:38:22, lo0
C   4000::/64 [0/0]
    via ::, 00:31:55, gigabitethernet0/0/1
L   4000::2/128 [0/0]
    via ::, 00:31:53, lo0
```

**Note:**

- The viewing method of Device1 is the same as that of Device2, so the viewing process is omitted.

**Step 3:** Enable the IPv6 multicast forwarding globally, configure PIM-SMv6 SSM globally and the multicast group range of the SSM service is FF3X::/32. On the interfaces, enable the multicast protocol PIM-SMv6. The interface gigabitethernet0/0/1 of Device2 runs MLDv2.

#Configure Device1.

Enable the IPv6 multicast forwarding globally, configure the PIM-SMv6 SSM globally and enable the multicast protocol PIM-SMv6 on the interface.

```
Device1(config)#ipv6 multicast-routing
Device1(config)#ipv6 pim ssm default
Device1(config)#interface gigabitethernet0/0/0
Device1(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/0)#exit
Device1(config)#interface gigabitethernet0/0/1
Device1(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/1)#exit
Device1(config)#interface gigabitethernet0/0/2
Device1(config-if-gigabitethernet0/0/2)#ipv6 pim sparse-mode
```

```
Device1(config-if-gigabitethernet0/0/2)#exit
```

#Configure Device2.

Enable the IPv6 multicast forwarding globally, configure the PIM-SMv6 SSM globally, enable the multicast protocol PIM-SMv6 on the related interfaces, and run MLDv2 on the interface gigabitethernet0/0/1.

```
Device2(config)#ipv6 multicast-routing
Device2(config)#ipv6 pim ssm default
Device2(config)#interface gigabitethernet0/0/0
Device2(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device2(config-if-gigabitethernet0/0/0)#exit
Device2(config)#interface gigabitethernet0/0/1
Device2(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device2(config-if-gigabitethernet0/0/1)#ipv6 mld enable
Device2(config-if-gigabitethernet0/0/1)#exit
```

#View the MLD information of the interface gigabitethernet0/0/1 on Device2.

```
Device2#show ipv6 mld interface gigabitethernet 1
Interface gigabitethernet0/0/1 (Index 23)
 MLD Enabled, Active
 Querier: fe80::201:2ff:fe03:406 (Self)
 Default version: 2
 Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  Query response time is 10 seconds
  Last member query response interval is 1 seconds
        Last member query count is 2
  Group Membership interval is 260 seconds
        Robustness variable is 2
```

**Step 4:** Enable the MLD SSM mapping on Device2 and configure the MLD SSM mapping rule so that Receiver1 and Receiver2 can only receive the multicast packets sent by Source1.

#Configure Device2.

Enable the MLD SSM mapping, configure the multicast group range of the MLD SSM as FF3E::/64, and the multicast source address is 1000::a.

```
Device2(config)#ipv6 access-list extended 7001
Device2(config-std-nacl)#permit ipv6 any ff3e::/64
Device2(config-std-nacl)#exit
Device2(config)#ipv6 mld ssm-map enable
```

```
Device2(config)#ipv6 mld ssm-map static 7001 1000::a
```

**Step 5:** Check the result.

# Receiver1 sends the MLDv2 member report packet of the specified source group to add to the multicast group FF3E::1 and the specified multicast source is 2000::a; Receiver2 sends the MLDv1 member report packet to add to the multicast group FF3E::2.

#Source1 and Source2 both send the multicast service packets with multicast groups FF3E::1 and FF3E::2.

#View the multicast member table of Device2.

```
Device2#show ipv6 mld groups
MLD Connected Group Membership
Total 2 Connected Groups
Group        Interface        Uptime     Expires  V1-Expires Last Reporter
ff3e::1      gigabitethernet0/0/1  00:00:33   not used not used   fe80::a
ff3e::2      gigabitethernet0/0/1  00:00:33   not used not used   fe80::b

Device2#show ipv6 mld groups detail
MLD Connected Group Membership
Total 2 Connected Groups
Group        Interface        Uptime     Expires  V1-Expires Last Reporter
ff3e::1      gigabitethernet0/0/1  00:00:36   not used not used   fe80::a
 Group mode : Include
 TIB-A Count: 1
 TIB-B Count: 0

TIB-A
Source list: (R - Remote, M - SSM Mapping)
 Source                          Uptime     Expires  Flags
2000::a                         00:00:36   00:03:49 R


ff3e::2      gigabitethernet0/0/1  00:00:36   not used not used   fe80::b
Group mode : Include
TIB-A Count: 1
TIB-B Count: 0

TIB-A
Source list: (R - Remote, M - SSM Mapping)
```

```
Source                          Uptime    Expires  Flags
1000::a                         00:00:36  00:03:45 RM
```

#View the multicast route table of Device2.

```
Device2#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 VRF Name: Default
Total 0 (*,*,RP) entry
Total 0 (*,G) entry
Total 2 (S,G) entries
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(2000::a, ff3e::1)
Up time: 00:01:36
KAT time: 00:01:54
RPF nbr: fe80::201:2ff:fe03:406
RPF idx: gigabitethernet0/0/0
SPT bit: FALSE
Flags:
JOIN DESIRED
Upstream State: JOINED
Local interface list:
gigabitethernet0/0/1
Joined interface list:
Asserted interface list:
Outgoing interface list:
gigabitethernet0/0/1
Packet count 0

(1000::a, ff3e::2)
Up time: 00:01:36
KAT time: 00:01:54
RPF nbr: fe80::201:2ff:fe03:406
RPF idx: gigabitethernet0/0/0
SPT bit: FALSE
```

```
Flags:
JOIN DESIRED
Upstream State: JOINED
Local interface list:
 gigabitethernet0/0/1
Joined interface list:
Asserted interface list:
Outgoing interface list:
 gigabitethernet0/0/1
Packet count 0
```

#Receiver1 can only receive the multicast service packets sent by Source2; Receiver2 can only receive the multicast service packets sent by Source1.

**Note:**

- The viewing method of Device1 is the same as that of Device2, so the viewing process is omitted.
- MLD SSM mapping needs to be used with PIM-SMv6 SSM; the multicast group range in the MLD SSM mapping rule should belong to the PIM-SMv6 SSM multicast group range. IGMP SSM mapping mainly runs MLDv1 and cannot be upgraded to the receiver host of MLDv2 to provide the supporting for the SSM model.
- The MLD SSM mapping is invalid for the MLDv2 member report packet.

## 10.3.4. Configure MLD Multicast Group Filter

### Network Requirements

- The whole network runs the PIM-SMv6 protocol.
- Receiver is one receiver of the Device stub network.
- Run MLDv2 between Device and the stub network.
- Device interface gigabitethernet0/0/1 filters the multicast group; the range of the multicast groups Receiver is permitted to add is ff10::/16.

### Network Topology

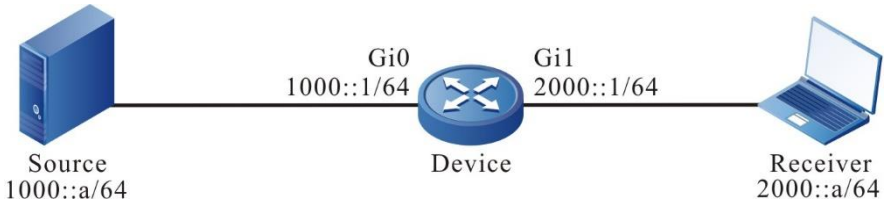


Figure 10-4 Networking of configuring IGMP multicast group filter

### Configuration Steps

**Step 1:** Configure the IPv6 address of the interface (omitted).

**Step 2:** Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the interface.

#Configure Device.

Globally enable the IPv6 multicast forwarding, enable the multicast protocol PIM-SMv6 on the related interfaces, and enable MLD on the interface of connecting Receiver.

```
Device#configure terminal
Device(config)#ipv6 multicast-routing
Device(config)#interface gigabitethernet0/0/0
Device(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device(config-if-gigabitethernet0/0/0)#exit
Device(config)#interface gigabitethernet0/0/1
Device(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device(config-if-gigabitethernet0/0/1)#ipv6 mld enable
Device(config-if-gigabitethernet0/0/1)#exit
```

#View the MLD information of Device interface gigabitethernet0/0/1.

```
Device#show ipv6 mld interface gigabitethernet 1
Interface gigabitethernet0/0/1 (Index 23)
 MLD Enabled, Active
 Querier: fe80::201:2ff:fe03:406 (Self)
 Default version: 2
 Querier parameter:
  Query interval is 125 seconds
  Querier timeout is 255 seconds
  Query response time is 10 seconds
 Last member query response interval is 1 seconds
 Last member query count is 2
 Group Membership interval is 260 seconds
 Robustness variable is 2
```

**Step 3:** Configure the multicast group filter on Device interface gigabitethernet0/0/1.

#Configure Device.

Configure the multicast group filter on Device interface gigabitethernet0/0/1; the range of the multicast groups Receiver is permitted to add is ff10::/16.

```
Device(config)#ipv6 access-list extended 7001
Device(config-std-nacl)#permit ipv6 any ff10::/16
Device(config-std-nacl)#exit
Device(config)#interface gigabitethernet0/0/1
Device(config-if-gigabitethernet0/0/1)#ipv6 mld access-group 7001
Device(config-if-gigabitethernet0/0/1)#exit
```

**Step 4:** Check the result.

#Receiver sends the IGMPv2 member report packet to add to multicast group FF10::1 and FF11::1.

#Source sends the multicast packets with multicast group FF10::1 and FF11::1.

#View the multicast member table of Device.

```
Device#show ipv6 mld groups
MLD Connected Group Membership
Total 1 Connected Groups
Group        Interface        Uptime    Expires  V1-Expires Last Reporter
ff10::1      gigabitethernet0/0/1  01:06:32   00:04:15 00:04:15   fe80::b
```

#View the multicast route table of Device.

```
Device#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer


(*, ff10::1)
Up time: 00:01:00
RP: ::
RPF nbr: ::
RPF idx: None
Flags:
Upstream State: NOT JOINED
  Local interface list:
    gigabitethernet0/0/1
  Joined interface list:
  Asserted interface list:

(1000::a, ff10::1)
Up time: 00:00:06
KAT time: 00:03:24
RPF nbr: ::
```

RPF idx: None
SPT bit: TRUE
Flags:
 JOIN DESIRED
 COULD REGISTER
Upstream State: JOINED
 Local interface list:
  gigabitethernet0/0/1
 Joined interface list:
  register_vif0
 Asserted interface list:
 Outgoing interface list:
register_vif0
gigabitethernet0/0/1
 Packet count 1

(1000::a, ff10::1, rpt)
Up time: 00:00:06
RP: ::
Flags:
 RPT JOIN DESIRED
 RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
 Local interface list:
 Pruned interface list:
 Outgoing interface list:

(1000::a, ff11::1)
Up time: 00:00:06
KAT time: 00:03:24
RPF nbr: ::
RPF idx: None
SPT bit: TRUE
Flags:
 JOIN DESIRED
 COULD REGISTER
Upstream State: JOINED

```
  Local interface list:
  Joined interface list:
    register_vif0
  Asserted interface list:
  Outgoing interface list:
    register_vif0
  Packet count 1


(1000::a, ff11::1, rpt)
Up time: 00:00:06
RP: ::
Flags:
  RPF SGRPT XG EQUAL
Upstream State: RPT NOT JOINED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
```

#Receiver can only receive the multicast service packets with multicast group FF10::1 sent by Source.

**Note:**

- To filter based on multicast source group, use the command **ipv6 mld access-group** to realize, and configure the corresponding source address in the associated ACL. For example, permit ipv6 1000::/16 ff10::/16 indicates permitting the source group in the group range FF10::/16 and the specified source range 1000::/16 to add. When using the function, it is required that the interface runs MLDv2.

# 11. IPV6 MULTICAST BASICS

## 11.1. Overview

IPv6 multicast basics is the basis of running the IPv6 multicast protocol and the common part of all multicast protocols. No matter which multicast route protocol runs, we first need to enable the IPv6 multicast forwarding function so that the device can forward the multicast service packets.

Basic Function Configuration of IPv6 Multicast

Table 11-1 Basic function configuration list of IPv6 multicast

| Configuration task | |
|---|---|
| Enable the IPv6 multicast forwarding | Enable the IPv6 multicast forwarding |

### 11.1.1. Enable IPv6 Multicast Forwarding

IPv6 multicast forwarding is the basic module of the multicast forwarding. The device can forward the IPv6 multicast service packets only after enabling the IPv6 multicast forwarding function. Both the general IPv6 multicast forwarding and IPv6 multicast fast forwarding are controlled by whether to enable the IPv6 multicast forwarding.

IPv6 multicast fast forwarding is one IPv64 fast multicast forwarding technology designed to improve the forwarding performance of the service packets. It completes the route selection and service processing for a time, so as to reduce the resource consumption caused by the switching between the internal tasks of the system and the packet cache management. At last, improve the data forwarding performance of the whole system.

#### Configuration Condition

Before configuring the IPv6 multicast forwarding function, first complete the following task:

- Configure the IPv6 address of the interface, making the neighboring node network layer reachable;
- Configure any unicast routing protocol, making the routes in the domain reachable;
- Configure any multicast routing protocol.

#### Enable IPv6 Multicast Forwarding

The device can forward the IPv6 multicast service packets only after enabling the IPv6 multicast forwarding function.

Table 11-2 Enable the IPv6 multicast forwarding

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable the IPv6 multicast forwarding | **ipv6 multicast-routing** [ **vrf** *vrf-name* ] | Mandatory<br>By default, the IPv6 multicast forwarding is not enabled. |

## 11.1.2. Configure IPV6 Muticast Forwarding Rules

### Configuration Conditions

Before configuring the IPv6 multicast forwarding rules, first complete the following tasks:

- Configure the IPv6 address of the interface so that each neighboring node can reach the network layer;
- Configure any IPv6 unicast routing protocol to make intra domain routing reachable;
- Enable IPv6 multicast forwarding;
- Configure any IPv6 multicast routing protocol.

### Configure IPV6 Multicast Forwarding Management Boundary

The main function of IPv6 multicast forwarding management boundary is to filter IPv6 multicast service packets. After configuring the management boundary, the device can filter IPv6 multicast service packets. Only IPv6 multicast services allowed by ACL can pass through.

Table 11-3 Configure the IPv6 multicast forwarding management boundary

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Configure the IPv6 multicast forwarding management boundary | **ipv6 multicast boundary**<br>{ *access-list-number* \| *access-list-name* } | Mandatory<br>By default, do not configure the IPv6 multicast forwarding management boundary. |

### Configure IPV6 Multicast Route Table Limit

Configure the maximum entries of IPv6 Multicast routing table. After exceeding the maximum entries of IPv6 multicast routing table, no new IPv6 multicast routing table will be created.

Table 11-4 Configure IPV6 multicast route table limit

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure IPV6 multicast route table limit | **ipv6 multicast route-limit** *number-value* [ **vrf** *vrf-name* ] | Optional<br>By default, the maximum entries of the multicast route table is 8192. |

## Configure TTL Threshold of IPV6 Multicast Interface

The ingress interface TTL threshold of IPv6 multicast: Only the IPv6 multicast service packet with TTL greater than the threshold can be accepted, and the IPv6 multicast data packet with TTL less than or equal to this threshold will be discarded.

The egress interface TTL threshold of IPv6 multicast: Only the IPv6 multicast service packet that are still greater than the threshold after TTL minus 1 can be forwarded, and the IPv6 multicast data packet with TTL less than or equal to this threshold will be discarded.

Table 11-5 Configure the TTL threshold of the IPv6 multicast interface

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Configure the ingress interface TTL threshold of IPv6 multicast | **ipv6 multicast in-threshold** *number-value* | Optional<br>By default, the threshold of the IPv6 multicast ingress interface is 0. |
| Configure the egress interface TTL threshold of IPv6 multicast | **ipv6 multicast out-threshold** *number-value* | Optional<br>By default, the threshold of the IPv6 multicast egress interface is 0. |

## Monitoring and Maintaining of IPv6 Multicast Basics

Table 11-6 Monitoring and maintaining of IPv6 multicast basics

| Command | Description |
|---|---|
| **clear ipv6 mcache[** [ **source** *source-ipv6-address* ] [ **group** *group-ipv6-address* ] [ **vrf** *vrf-name* ]]\|[**all**]] | Clear the multicast core route table |
| **show ipv6 mcache** [ **source** *source-ipv6-address* ] [ **group** *group-ipv6-address* ] [ **vrf** *vrf-name* ] | Display the multicast core route table information |
| **show ipv6 mcast fib** [ **source** *source-ipv6-address* ] [ **group** *group-ipv6-address* ][ **vrf** *vrf-name*\| **vrf-id** *vrf-id* ] | Display the multicast fast forwarding table information |
| **show ipv6 mvif** [ **vrf** *vrf-name* ] | Display the multicast virtual interface information |

# 12. PIM-SMV6

## 12.1. Overview

IPv6 PIM protocol and IPv4 PIM protocol have the same behaviors except the IP address structure in the packet. Refer to the brief introduction of PIM-SM.

## 12.2. PIM-SMv6 Function Configuration

Table 12-1 PIM-SMv6 function configuration list

| Configuration Task | |
|---|---|
| Configure the PIM-SMv6 basic functions | Enable the PIM-SMv6 protocol |
| Configure the PIM-SMv6 aggregation router | Configure C-RP |
| | Configure static RP |
| Configure the PIM-SMv6 bootstrap router | Configure C-BSR |
| | Configure the BSR edge |
| Configure PIM-SMv6 multicast source registration | Configure the RP reachability check |
| | Configure the sending rate of the register packets |
| | Configure sending rate of the register stop packets |
| | Configure the source address of the register packet |
| | Configure register packet filter |
| Configure PIM-SMv6 neighbor parameters | Configure the period of sending the Hello packets |
| | Configure the keepalive time of the neighbor |
| | Configure the neighbor filter |

| Configuration Task | |
|---|---|
| | Configure the DR priority |
| Configure PIM-SMv6 SPT switching | Configure the SPT switching condition |
| Configure IPv6 PIM-SSM | Configure IPv6 PIM-SSM |

## 12.2.1. Configure PIM-SMv6 Basic Functions

### Configuration Conditions

Before configuring PIM-SMv6, first complete the following task:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable

### Enable PIM-SMv6 Protocol

Table 12-2 Enable the PIM-SMv6 protocol

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enable the IPv6 multicast forwarding | **ipv6 multicast-routing** [ **vrf** *vrf-name* ] | Mandatory<br>By default, the IPv6 multicast forwarding is not enabled. |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Enable the PIM-SMv6 protocol | **ipv6 pim sparse-mode** | Either<br>By default, PIM-SMv6 is disabled on the interface. |
| | **ipv6 pim sparse-mode passive** | |

**Note:**

- After enabling the PIM-SMv6 function, all PIM-SMv6 configurations can take effect.

## 12.2.2. Configure PIM-SMv6 Aggregation Router

### Configuration Condition

Before configuring RP, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Enable the PIM-SMv6 protocol

### Configure C-RP

RP is generated by the C-RO election. After BSR is elected, all C-RPs (Candidate-Rendezvous Point) regularly unicast the C-RP packet to BSR. BSR integrates the C-RP information and transmits the information to all devices in the PIM-SMv6 domain via the bootstrap packet.

Table 12-3 Configure C-RP

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure C-RP | **ipv6 pim rp-candidate** *interface-name* [ [ *priority-value* [ *interval-value* [ **group-list** { *access-list-number* \| *access-list-name* } ] ] ] \| [ **group-list** { *access-list-number* \| *access-list-name* } ] ] [ **vrf** *vrf-name* ] | Mandatory<br>By default, there is no C-RP. |

**Note:**

- RP election rules:
- For the group range of the C-RP service, perform the longest matching of the mask.
- If the longest matching of the mask has multiple C-RPs, compare the C-RP priority. The smaller the value, the high the priority. The one with highest priority wins.
- If there are multiple C-RPs with highest priority, perform the HASH calculation for the C-RP address and group. The one with the largest HASH value wins.
- If there are multiple RPs with the largest HASH, the C-RP with the largest IPv6 address wins.

### Configure Static RP

For the simple PIM-SMv6 network, it is suggested to use the static RP. If using the static RP, do not need to perform the BSR configuration, eliminating the frequent interacting between RP and BSR, so as to save the network bandwidth.

Table 12-4 Configure static RP

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the static RP | **ipv6 pim rp-address** *ipv6-address* [ *access-list-name* \| *access-list-number* ] [ **override** ] [ **vrf** *vrf-name* ] | Mandatory<br>By default, there is no static RP. |

**Note:**

- All devices in the same PIM-SMv6 domain should be configured with the same static RP.

## 12.2.3. Configure PIM-SMv6 Bootstrap Router

### Configuration Conditions

Before configuring BSR, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Enable the PIM-SMv6 protocol

### Configure C-BSR

In one PIM-SMv6 domain, there should be the unique BSR. Multiple C-BSRs (Candidate-Bootstrap Router) elects to generate the unique BSR via the bootstrap packet.

Table 12-5 Configure C-BSR

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure C-BSR | **ipv6 pim bsr-candidate** *interface_name* [ *hash-mask-length* [ *priority-value* ] ] [ **vrf** *vrf-name* ] | Mandatory<br>By default, there is no C-BSR. |

**Note:**

- BSR election rules:
- Compare the priorities. The larger the value, the higher the priority. The one with highest priority wins.
- If the priority is the same, the one with the largest IPv6 address wins.

### Configure BSR Border

BSR is responsible for collecting the C-RP information and transmits the information to all devices in the PIM-SMv6 domain via the bootstrap packet. The BSR range is the range of the multicast domain. The bootstrap packet cannot pass the interface configured with the BSR border. The devices out of the multicast domain range cannot take part in the forwarding of the multicast service packet in the multicast domain, so as to realize the dividing of the multicast domain.

Table 12-6 Configure the BSR border

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the BSR border | **ipv6 pim bsr-border** | Mandatory<br>By default, there is no multicast border. |

## 12.2.4. Configure PIM-SMv6 Multicast Source Register

### Configuration Condition

Before configuring the multicast source register, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Enable the PIM-SMv6 protocol

### Configure RP Reachability Check

Before source DR sends the register packet to RP, first perform the RP reachability check. If finding that the RP route is not reachable, do not register to RP, so as to reduce the cost of the DR.

Table 12-7 Configure the RP reachability check

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the RP reachability check | **ipv6 pim register-rp-reachability** [ **vrf** *vrf-name* ] | Mandatory<br>By default, before performing the PIM register, do not check the RP reachability. |

**Note:**

- To reduce the cost of the source DR, it is suggested to configure the command on the source DRs of all PIM-SMv6s.

### Configure Sending Rate of Register Packets

When the source DR receives the multicast packet, encapsulate the multicast packet to the register packet and send to RP for source register until the registration is complete..

When the source DR does not complete the multicast source register and the multicast flow is large, generate lots of register packets, which increase the load of the RP device. Even RP cannot work normally. Source DR does not need to transmit all register packets of one flow to RP, so configuring the rate of sending the register packets at the source DR not only can reach the purpose of source registration, but also can reduce the RP load.

Table 12-8 Configure the rate of sending the register packet

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the rate of sending the register packet | **ipv6 pim register-rate-limit** *rate-limit-value* [ **vrf** *vrf-name* ] | Mandatory<br>By default, do not limit the rate of sending the register packet. |

**Note:**

- To reduce the RP load, it is suggested to configure the rate of sending the source register packets on all source DRs.

### Configure Sending Rate of Register Stop Packets

After RP receives the register packet of the source DR, send the register stop packet to the source DR to complete the registration. When the RP receives lots of register packets, it is necessary to reply all register packets (send register stop packet). In fact, there are lots of repeated packets in the register stop packets. You can limit the rate of sending the register stop packet on RP to reduce the cost of RP.

Table 12-9 Configure the rate of sending the register stop packet

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | configure terminal | - |
| Configure the rate of sending the register stop packet | ipv6 pim register-stop-rate-limit rate-limit-value [ vrf vrf-name ] | Mandatory<br>By default, do not limit the rate of sending the register stop packet. |

**Note:**

- To improve the robustness of the whole PIM-SMv6 network, it is suggested to limit the rate of the source register stop packet on all RPs.

### Configure Source Address of Register Packet

When the source DR performs the source register, the source address of the register packet uses the IPv6 address of the register interface automatically registered by the system. The command can specify the source address of the register packet as the IPv6 address of one interface on the device to meet some special demand of the network.

Table 12-10 Configure the source address of the register packet

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the source address of the register packet | **ipv6 pim register-source interface** *interface-name* [ **vrf** *vrf-name* ] | Mandatory<br>By default, use IPv6 address of the register interface automatically registered by the system as the source address of the register packet. |

### Configure Register Packet Filter

To prevent the source register attack, you can use ACL on RP to perform the multicast source filter for the register packet. Only the multicast source permitted by ACL can register successfully on RP.

Table 12-11 Configure the register packet filter

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the register packet filter | **ipv6 pim accept-register list** { *access-list-number* \| *access-list-name* } [ **vrf** *vrf-name* ] | Mandatory<br>By default, do not filter the register packet. |

## 12.2.5. Configure PIM-SMv6 Neighbor Parameters

### Configuration Condition

Before configuring the PIM-SMv6 neighbor parameters, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Enable the PIM-SMv6 protocol

### Configure Sending Period of Hello Packets

The interface enabled with the PIM-SMv6 protocol periodically sends the Hello packets to set up and maintain the PIM neighbor.

Table 12-12 Configure the period of sending the Hello packet

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the period of sending the Hello packet | **ipv6 pim hello-interval** *interval-value* | Optional<br>By default, the period of sending the Hello packet is 30s. |

### Configure Neighbor Keepalive Time

When the interface receives the Hello packets of one neighbor, record the holdtime carried in the Hello packet as the keepalive time of the neighbor. If not receiving the Hello packet of the neighbor within the keepalive time, it is regarded that the neighbor becomes invalid.

Table 12-13 Configure PIM-SMv6 neighbor keepalive time

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure PIM-SMv6 neighbor keepalive time | **ipv6 pim hello-holdtime** *holdtime-value* | Optional<br>By default, the keepalive time of the PIM-SMv6 neighbor is 105s. |

### Configure Neighbor Filter

If there are many PIM neighbors in one subnet, you can use the neighbor filter function to set up the neighbor selectively, so as to save the resources of the device.

Table 12-14 Configure the neighbor filter

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the neighbor filter | **ipv6 pim neighbor-filter** { *access-list-number* \| *access-list-name* } | Mandatory<br>By default, do not enable the neighbor filter function. |

### Configure DR Priority

DR plays one important role in the PIM-SMv6 network, so selecting the appropriate DR is important. You can select the appropriate device as DR by configuring the DR priority.

One PIM-SMv6 subnet only permits one DR. According to the function, DR can be divided to source DR and receiving DR.

The main function of the source DR is to perform the source register to RP.

The main function of the receiving DR is to add to RP and set up the switching of RPT and SPT.

Table 12-15 Configure the DR priority

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter interface configuration mode | **interface** *interface-name* | - |
| Configure the DR priority | **ipv6 pim dr-priority** *priority-value* | Optional<br>By default, the DR priority is 1. |

**Note:**

DR election rules:

- Compare the priorities. The larger the value, the higher the priority. The one with highest priority wins.
- If the priority is the same, the one with the largest IPv6 address wins.

## 12.2.6. Configure PIM-SMv6 SPT Switching

### Configuration Condition

Before configuring SPT, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Enable the PIM-SMv6 protocol

### Configure SPT Switching Condition

The receiving end DR does not know the address of the multicast source, so it can only add to RP to form RPT. The source DR performs the source register to RP and form the source tree between source DR and RP. At first, the direction of the multicast flow is from multicast source to RP and then from RP to the receiver. When the receiving end DR receives the first multicast packet, it performs adding to multicast source, forms SPT, and performs the pruning for RPT. This is called SPT switching.

The command is to configure the SPT switching condition at the receiving end DR.

Table 12-16 Configure the SPT switching condition

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure the SPT switching condition | **ipv6 pim spt-threshold** { **infinity \|** *threshold* [ **group-list** {*access-list-number* \| *access-list-name* } ] [ **vrf** *vrf-name* ] | Mandatory<br>By default, all multicast groups perform the SPT switching. |

**Caution:**

- Do not configure SPT never-switching on RP. Otherwise, it may result in the failure of the multicast forwarding.

## 12.2.7. Configure IPv6 PIM-SSM

IPv6 PIM-SSM is one subset of PIM-SMv6. In IPv6 PIM-SSM, do not need RP, BSR or RPT, and there is no SPT switching, but the receiving end DR directly adds to multicast source and sets up the shortest path tree (SPT) with source as root.

### Configuration Condition

Before configuring IPv6 PIM-SSM, first complete the following tasks:

- Configure the network layer address of the interface, making the neighboring node network layer reachable
- Configure any unicast route protocol, reaching the intra-domain route reachable
- Enable the PIM-SMv6 protocol on all interfaces that need multicast route forwarding

### Configure IPv6 PIM-SSM

Table 12-17 Configure IPv6 PIM-SSM

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Configure PIM-SSM | **ipv6 pim ssm** { **default** \| **range** { *access-list-number* \| *access-list-name* } } [ **vrf** *vrf-name* ] | Mandatory<br>By default, the SSM function is disabled. |

**Caution:**

- When using IPv6 PIM-SSM, the receiving end should enable MLDv2.
- When the receiver cannot be upgraded to MLDv2, you can use the IGMP SSM Mapping function to cooperate with IPv6 PIM-SSM.
- Ensure that the SSM multicast group address ranges configured on all devices in the domain are consistent. Otherwise, it may result in the abnormality of IPv6 PIM-SS.

## 12.2.8. Configure PIM6-SM BFD

### Configuration Conditions

Before configuring IPv6 PIM-SM BFD, first complete the following tasks:

- Configure the network layer address of the interface so that each neighboring node can reach the network layer;
- Configure any unicast routing protocol to make the intra-domain routing reachable.

### Configure IPv6 PIM-SM BFD

Table 12-18 Configure PIM-SM BFD

| Step | Command | Description |
|---|---|---|
| Enter global configuration mode | **configure terminal** | - |
| Enter the interface configuration mode | **interface** *interface-name* | - |
| Enable IPv6 PIM-SM BFD | **ipv6 pim bfd** | By default, do not enable the IPv6 PIM-SM BFD function. |

## 12.2.9. PIM-SMv6 Monitoring and Maintaining

Table 12-19 PIM-SMv6 monitoring and maintaining

| Command | Description |
|---|---|
| **clear ipv6 pim bsr rp-set** [ **vrf** *vrf-name* ] | Clear the RP set information of PIM-SMv6 |
| **clear ipv6 pim mroute** [ *group-address* [ *source-address* ] ] [ **vrf** *vrf-name* ] | Clear the multicast route information of PIM-SMv6 |
| **clear ipv6 pim stat** [ [ **interface** *interface-name* \| [ **all_interface** ] ] \| [ **vrf** *vrf-name* ] ] | Clear the statics information of the PIM-SMv6 protocol packets |

| Command | Description |
|---|---|
| **show ipv6 pim bsr-router** [ **vrf** *vrf-name* ] | Display the PIM-SMv6 bootstrap route information |
| **show ipv6 pim interface** [ *interface-name* **detail \| detail** ] [ **vrf** *vrf-name* ] | Display the PIM-SMv6 interface information |
| **show ipv6 pim local-members** *interface-name* [ **vrf** *vrf-name* ] | Display the PIM-SMv6 local group member information |
| **show ipv6 pim mroute** [ **active** \| **proxy** \| **ssm** [ **active** ] \| **group** *group-ipv6-address* [ **source** *source-ipv6-address* \| **active** ] \| **source** *source-ipv6-address* ] [ **vrf** *vrf-name* ] | Display the PIM-SMv6 multicast route table information |
| **show ipv6 pim neighbor** [ **detail** ] [ **vrf** *vrf-name* ] | Display the PIM-SMv6 neighbor information |
| **show ipv6 pim nexthop** [ *ipv6-address* ] [ **vrf** *vrf-name* ] | Display the PIM-SMv6 next-hop router information |
| **show ipv6 pim rp mapping** [ **vrf** *vrf-name* ] | Display the PIM-SMv6 RP information |
| **show ipv6 pim rp-hash** *group-address* [ **vrf** *vrf-name* ] | Display the RP information of the multicast group mapping |
| **show ipv6 pim statistics** [ **vrf** *vrf-name* ] | Display the statistics information of the PIM-SMv6 protocol packets |

## 12.3. PIM-SMv6 Typical Configuration Example

### 12.3.1. Configure PIM-SMv6 Basic Functions

#### Network Requirements

- The whole network runs the PIM-SMv6 protocol.
- Receiver1 and Receiver2 are the two receivers of Device3 stub network.
- Device1 and Device2 are C-BSR and C-RP.
- Run MLDv2 between Device3 and the stub network.

## Network Topology

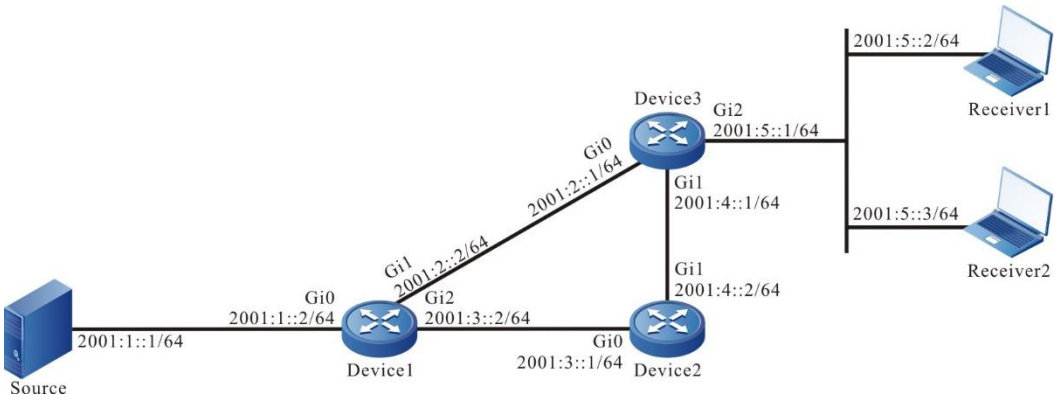


Figure 12-1 Networking of configuring PIM-SMv6 basic functions

## Configuration Steps

**Step 1:** Configure the IPv6 address of the interface. (omitted)

**Step 2:** Enable the unicast route protocol OSPFv3 so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface gigabitethernet0/0/0
Device1(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/0)#exit
Device1(config)#interface gigabitethernet0/0/1
Device1(config-if-gigabitethernet0/0/1)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/1)#exit
Device1(config)#interface gigabitethernet0/0/2
Device1(config-if-gigabitethernet0/0/2)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/2)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface gigabitethernet0/0/0
Device2(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
```

```
Device2(config-if-gigabitethernet0/0/0)#exit
Device2(config)#interface gigabitethernet0/0/1
Device2(config-if-gigabitethernet0/0/1)#ipv6 router ospf 100 area 0
Device2(config-if-gigabitethernet0/0/1)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface gigabitethernet0/0/0
Device3(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/0)#exit
Device3(config)#interface gigabitethernet0/0/1
Device3(config-if-gigabitethernet0/0/1)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/1)#exit
Device3(config)#interface gigabitethernet0/0/2
Device3(config-if-gigabitethernet0/0/2)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/2)#exit
Device3(config)#interface gigabitethernet0/0/3
Device3(config-if-gigabitethernet0/0/3)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/3)#exit
```

#View the route table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management


L   ::1/128 [0/0]
    via ::, 2w6d:04:39:46, lo0
O   2001:1::/64 [110/2]
    via fe80::201:7aff:fe62:bb7e, 00:00:24, gigabitethernet0/0/0
C   2001:2::/64 [0/0]
    via ::, 00:01:05, gigabitethernet0/0/0
L   2001:2::1/128 [0/0]
```

```
    via ::, 00:01:04, lo0
O   2001:3::/64 [110/2]
    via fe80::201:7aff:fe62:bb7e, 00:00:24, gigabitethernet0/0/0
          [110/2]
    via fe80::201:7aff:fec0:525a, 00:00:04, gigabitethernet0/0/1
C   2001:4::/64 [0/0]
    via ::, 00:00:49, gigabitethernet0/0/1
L   2001:4::1/128 [0/0]
    via ::, 00:00:48, lo0
C   2001:5::/64 [0/0]
    via ::, 00:00:43, gigabitethernet0/0/2
L   2001:5::1/128 [0/0]
    via ::, 00:00:42, lo0
C   2001:6::/64 [0/0]
    via ::, 00:00:43, gigabitethernet0/0/3
L   2001:6::1/128 [0/0]
    via ::, 00:00:42, lo0
```

**Note:**

- The viewing method of Device1 and Device2 is the same as that of Device3, so the viewing process is omitted.

**Step 3:** Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the interface.

#Configure Device1.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the related interfaces.

```
Device1(config)#ipv6 multicast-routing
Device1(config)#interface gigabitethernet0/0/0
Device1(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/0)#exit
Device1(config)#interface gigabitethernet0/0/1
Device1(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/1)#exit
Device1(config)#interface gigabitethernet0/0/2
Device1(config-if-gigabitethernet0/0/2)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/2)#exit
```

#Configure Device2.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the related interfaces.

```
Device2(config)#ipv6 multicast-routing
Device2(config)#interface gigabitethernet0/0/0
Device2(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device2(config-if-gigabitethernet0/0/0)#exit
Device2(config)#interface gigabitethernet0/0/1
Device2(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device2(config-if-gigabitethernet0/0/1)#exit
```

#Configure Device3.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the related interfaces.

```
Device3(config)#ipv6 multicast-routing
Device3(config)#interface gigabitethernet0/0/0
Device3(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device3(config-if-gigabitethernet0/0/0)#exit
Device3(config)#interface gigabitethernet0/0/1
Device3(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device3(config-if-gigabitethernet0/0/1)#exit
Device3(config)#interface gigabitethernet0/0/2
Device3(config-if-gigabitethernet0/0/2)#ipv6 pim sparse-mode
Device3(config-if-gigabitethernet0/0/2)#exit
Device3(config)#interface gigabitethernet0/0/3
Device3(config-if-gigabitethernet0/0/3)#ipv6 pim sparse-mode
Device3(config-if-gigabitethernet0/0/3)#exit
```

#View the information of the interface enabled with the PIM-SMv6 protocol on Device3 and the PIM-SMv6 neighbor information.

```
Device3#show ipv6 pim interface
PIM6 Interface Table:
PIM6 VRF Name: Default
Total 5 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Interface      VIF   Ver/  VIF   Nbr   DR    BSR   CISCO   Neighbor
                     Index  Mode  Flag  Count  Pri   Border Neighbor Filter
```

```
register_vif0   2     v2/S   UP
Address : fe80::201:7aff:fe5e:6d2d   Global Address: ::

gigabitethernet0/0/0        1     v2/S   UP   1    1    FALSE  FALSE
Address  :  fe80::201:7aff:fe5e:6d2d       Global  Address:  2001:2::1              DR:
fe80::201:7aff:fe62:bb7e

gigabitethernet0/0/1        3     v2/S   UP   1    1    FALSE  FALSE
Address  :  fe80::201:7aff:fe5e:6d2e       Global  Address:  2001:4::1              DR:
fe80::201:7aff:fec0:525a

gigabitethernet0/0/2        4     v2/S   UP   0    1    FALSE  FALSE
Address  :  fe80::201:7aff:fe5e:6d2f       Global  Address:  2001:5::1              DR:
fe80::201:7aff:fe5e:6d2f

gigabitethernet0/0/3        5     v2/S   UP   0    1    FALSE  FALSE
Address  :  fe80::201:7aff:fe5e:6d30       Global  Address:  2001:6::1              DR:
fe80::201:7aff:fe5e:6d30

Device3#show ipv6 pim neighbor
PIM6 Neighbor Table:
PIM6 VRF Name: Default
Total 2 Neighbor entries

Neighbor              Interface      Uptime/Expires     Ver   DR
Address                                                       Priority/Mode
fe80::201:7aff:fe62:bb7e gigabitethernet0/0/0          00:04:01/00:01:29   v2    1 / DR
fe80::201:7aff:fec0:525a gigabitethernet0/0/1          00:04:03/00:01:39   v2    1 / DR
```

**Note:**

- The viewing methods of Device1 and Device2 are the same as that of Device3, so the viewing process is omitted.

**Step 4:** Enable MLD on gigabitethernet0/0/2 and gigabitethernet0/0/3 of Device3.

#Configure Device3.

Enable MLD on gigabitethernet0/0/2 and gigabitethernet0/0/3 of Device3.

```
Device3(config)#interface gigabitethernet0/0/2
Device3(config-if-gigabitethernet0/0/2)#ipv6 mld enable
Device3(config-if-gigabitethernet0/0/2)#exit
Device3(config)#interface gigabitethernet0/0/3
```

```
Device3(config-if-gigabitethernet0/0/3)#ipv6 mld enable
Device3(config-if-gigabitethernet0/0/3)#exit
```

#Query the MLD information of Device3 interface gigabitethernet0/0/2 and gigabitethernet0/0/3.

```
Device3#show ipv6 mld interface
Interface gigabitethernet0/0/2 (Index 11)
 MLD Enabled, Active
 Querier: fe80::201:7aff:fe5e:6d2f (Self)
 Default version: 2
 Querier parameter:
   Query interval is 125 seconds
   Querier timeout is 255 seconds
   Query response time is 10 seconds
   Last member query response interval is 1 seconds
   Last member query count is 2
   Group Membership interval is 260 seconds
   Robustness variable is 2
Interface gigabitethernet0/0/3 (Index 12)
 MLD Enabled, Active
 Querier: fe80::201:7aff:fe5e:6d30 (Self)
 Default version: 2
 Querier parameter:
   Query interval is 125 seconds
   Querier timeout is 255 seconds
   Query response time is 10 seconds
   Last member query response interval is 1 seconds
   Last member query count is 2
   Group Membership interval is 260 seconds
   Robustness variable is 2
```

**Note:**

- You can configure the MLD version running on the interface via the command ipv6 mld version.

**Step 5:** Configure interface gigabitethernet0/0/1 of Device1 as C-BSR and C-RP, and configure interface gigabitethernet0/0/0 of Device2 as C-BSR and C-RP.

#Configure Device1.

Configure interface gigabitethernet0/0/1 of Device1 as C-BSR and C-RP; the priority of C-BSR is 200; the multicast group range of the C-RP service is FF10::/16.

```
Device1(config)#ipv6 pim bsr-candidate gigabitethernet0/0/1 10 200
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 any ff10::/16
Device1(config-v6-list)#exit
Device1(config)#ipv6 pim rp-candidate gigabitethernet0/0/1 group-list 7001
```

#Configure Device2.

Configure interface gigabitethernet0/0/0 of Device2 as C-BSR and C-RP; the priority of C-BSR is 0; the multicast group range of the C-RP service of Device2 is FF00::/8.

```
Device2(config)#ipv6 pim bsr-candidate gigabitethernet0/0/0
Device2(config)#ipv6 pim rp-candidate gigabitethernet0/0/0
```

#View the BSR and RP information of Device3.

```
Device3#show ipv6 pim bsr-router
PIM6v2 Bootstrap information
PIM6 VRF Name: Default
  BSR address: 2001:2::2
  BSR Priority: 200
  Hash mask length: 10
  Up time: 00:03:04
  Expiry time: 00:02:06
  Role: Non-candidate BSR
  State: Accept Preferred
Device3#show ipv6 pim rp mapping
PIM6 Group-to-RP Mappings Table:
PIM6 VRF Name: Default
Total 2 RP set entries
Total 2 RP entries

  Group(s): ff00::/8
  RP count: 1
    RP: 2001:3::1
      Info source: 2001:2::2, via bootstrap, priority 192
      Up time: 00:21:30
      Expiry time: 00:02:24

  Group(s): ff10::/16
  RP count: 1
```

```
RP: 2001:2::2
  Info source: 2001:2::2, via bootstrap, priority 192
  Up time: 00:04:31
  Expiry time: 00:02:24
```

**Caution:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.
- When configuring multiple C-BSRs in one multicast domain, first elect BSR according to the priority and the C-BSR with the largest priority is elected as BSR. When the priorities of C-BSRs are the same, the C-BSR with the largest ip address is elected as BSR.
- When configuring multiple C-RPs in one multicast domain and the service multicast group ranges are the same, calculate the RP of the multicast group G according to the hash algorithm.
- In the multicast domain, you can configure RP via the command **ipv6 pim rp-address**, but it is required that the static RP addresses configured on all devices in the multicast domain keep consistent.

**Step 7:** Check the result.

#PC1 and PC2 send the MLDv2 member report packet to add to multicast group FF10::1 and FF50::1respectively.

#Source sends the multicast packets with multicast group FF10::1, FF50::1.

#View the multicast member table of Device3.

```
Device3#show ipv6 mld groups
MLD Connected Group Membership
Total 2 Connected Groups
Group    Interface        Uptime    Expires  V1-Expires  Last Reporter
ff10::1  gigabitethernet0/0/2      00:00:09  00:04:13 not used    fe80::210:94ff:fe00:1
ff50::1     gigabitethernet0/0/3                  00:00:09     00:04:14    not used
fe80::210:94ff:fe00:2
```

#View the RP of multicast group FF10::1, FF50::1on Device3.

```
Device3#show ipv6 pim rp-hash ff10::1
  PIM6 VRF Name: Default
  RP: 2001:2::2
    Info source: 2001:2::2, via bootstrap
Device3#show ipv6 pim rp-hash ff50::1
  PIM6 VRF Name: Default
  RP: 2001:3::1
    Info source: 2001:2::2, via bootstrap
```

#View the multicast route table of Device3.

```
Device3#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 VRF Name: Default
Total 0 (*,*,RP) entry
Total 2 (*,G) entries
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer


(*, ff10::1)
Up time: 00:00:06
RP: 2001:2::2
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: gigabitethernet0/0/0
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    gigabitethernet0/0/2
  Joined interface list:
  Asserted interface list:


(2001:1::1, ff10::1)
Up time: 00:00:05
KAT time: 00:03:25
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: gigabitethernet0/0/0
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
```

```
  Outgoing interface list:
    gigabitethernet0/0/2
  Packet count 0

(2001:1::1, ff10::1, rpt)
Up time: 00:00:05
RP: 2001:2::2
Flags:
  RPT JOIN DESIRED
  RPF SGRPT XG EQUAL
Upstream State: NOT PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:

(*, ff50::1)
Up time: 00:00:06
RP: 2001:3::1
RPF nbr: fe80::201:7aff:fec0:525a
RPF idx: gigabitethernet0/0/1
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    gigabitethernet0/0/3
  Joined interface list:
  Asserted interface list:

(2001:1::1, ff50::1)
Up time: 00:00:05
KAT time: 00:03:27
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: gigabitethernet0/0/0
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
```

```
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet0/0/3
  Packet count 1

(2001:1::1, ff50::1, rpt)
Up time: 00:00:05
RP: 2001:3::1
Flags:
  RPT JOIN DESIRED
  PRUNE DESIRED
  RPF SGRPT XG EQUAL
Upstream State: PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    gigabitethernet0/0/3
```

#PC1 can only receive the multicast service packet with multicast group FF10::1 sent by Multicast Server. PC2 can only receive the multicast service packet with multicast group FF50::1 sent by Multicast Server.

**Note:**

- The viewing method of Device1 and Device2 is the same as that of Device3, so the viewing process is omitted.
- By default, the device enables the SPT switching.

## 12.3.2. Configure IPv6 PIM-SSM

### Network Requirements

- The whole network runs the IPv6 PIM-SSM protocol.
- PC is one receiver of Device3 stub network.
- Run MLDv2 between Device3 and the stub network.

## Network Topology

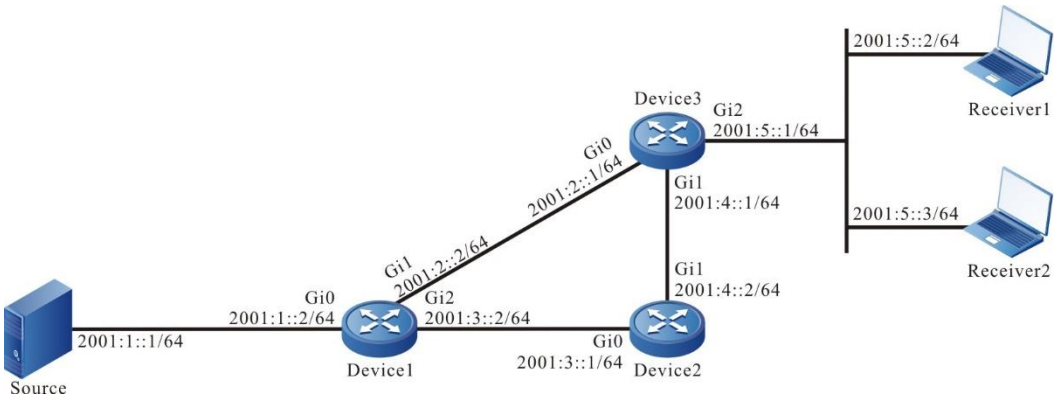


Figure 12-2 Networking of configuring IPv6 PIM-SSM

## Configuration Steps

**Step 1:** Configure VLAN, and add the port to the corresponding VLAN (omitted).

**Step 2:** Configure the IPv6 address of the interface. (omitted)

**Step 3:** Enable the unicast route protocol OSPFv3 so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface gigabitethernet0/0/0
Device1(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/0)#exit
Device1(config)#interface gigabitethernet0/0/1
Device1(config-if-gigabitethernet0/0/1)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/1)#exit
Device1(config)#interface gigabitethernet0/0/2
Device1(config-if-gigabitethernet0/0/2)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/2)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface gigabitethernet0/0/0
```

```
Device2(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
Device2(config-if-gigabitethernet0/0/0)#exit
Device2(config)#interface gigabitethernet0/0/1
Device2(config-if-gigabitethernet0/0/1)#ipv6 router ospf 100 area 0
Device2(config-if-gigabitethernet0/0/1)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface gigabitethernet0/0/0
Device3(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/0)#exit
Device3(config0)#interface gigabitethernet0/0/1
Device3(config-if-gigabitethernet0/0/1)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/1)#exit
Device3(config)#interface gigabitethernet0/0/2
Device3(config-if-gigabitethernet0/0/2)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/2)#exit
```

#View the route table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management


L   ::1/128 [0/0]
    via ::, 2w6d:04:39:46, lo0
O   2001:1::/64 [110/2]
    via fe80::201:7aff:fe62:bb7e, 00:00:24, gigabitethernet0/0/0
C   2001:2::/64 [0/0]
    via ::, 00:01:05, gigabitethernet0/0/0
L   2001:2::2/128 [0/0]
    via ::, 00:01:04, lo0
O   2001:3::/64 [110/2]
```

```
    via fe80::201:7aff:fe62:bb7e, 00:00:24, gigabitethernet0/0/0
          [110/2]
    via fe80::201:7aff:fec0:525a, 00:00:04, gigabitethernet0/0/1
C   2001:4::/64 [0/0]
    via ::, 00:00:49, gigabitethernet0/0/1
L   2001:4::1/128 [0/0]
    via ::, 00:00:48, lo0
C   2001:5::/64 [0/0]
    via ::, 00:00:43, gigabitethernet0/0/2
L   2001:5::1/128 [0/0]
    via ::, 00:00:42, lo0
```

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

**Step 4:** Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the interface.

#Configure Device1.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the related interfaces.

```
Device1(config)#ipv6 multicast-routing
Device1(config)#interface gigabitethernet0/0/0
Device1(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/0)#exit
Device1(config)#interface gigabitethernet0/0/1
Device1(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/1)#exit
Device1(config)#interface gigabitethernet0/0/2
Device1(config-if-gigabitethernet0/0/2)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/2)#exit
```

#Configure Device2.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the related interfaces.

```
Device2(config)#ipv6 multicast-routing
Device2(config)#interface gigabitethernet0/0/0
Device2(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device2(config-if-gigabitethernet0/0/0)#exit
Device2(config)#interface gigabitethernet0/0/1
```

```
Device2(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device2(config-if-gigabitethernet0/0/1)#exit
```

#Configure Device3.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the related interfaces.

```
Device3(config)#ipv6 multicast-routing
Device3(config)#interface gigabitethernet0/0/0
Device3(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device3(config-if-gigabitethernet0/0/0)#exit
Device3(config)#interface gigabitethernet0/0/1
Device3(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device3(config-if-gigabitethernet0/0/1)#exit
Device3(config)#interface gigabitethernet0/0/2
Device3(config-if-gigabitethernet0/0/2)#ipv6 pim sparse-mode
Device3(config-if-gigabitethernet0/0/2)#exit
```

#View the information of the interface enabled with the PIM-SMv6 protocol on Device3 and the PIM-SMv6 neighbor information.

```
Device3#show ipv6 pim interface
PIM6 Interface Table:
PIM6 VRF Name: Default
Total 4 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Interface      VIF   Ver/  VIF   Nbr   DR    BSR   CISCO   Neighbor
               Index Mode  Flag  Count Pri   Border Neighbor Filter
register_vif0  2     v2/S  UP
Address : fe80::201:7aff:fe5e:6d2d   Global Address: ::

gigabitethernet0/0/0        1     v2/S  UP    1     1     FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2d      Global Address: 2001:2::2          DR:
fe80::201:7aff:fe62:bb7e

gigabitethernet0/0/1        3     v2/S  UP    1     1     FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2e      Global Address: 2001:4::1          DR:
fe80::201:7aff:fec0:525a
```

```
gigabitethernet0/0/2        4     v2/S  UP   0    1    FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2f      Global Address: 2001:5::1              DR:
fe80::201:7aff:fe5e:6d2f
Device3#show ipv6 pim neighbor
PIM6 Neighbor Table:
PIM6 VRF Name: Default
Total 2 Neighbor entries

Neighbor              Interface      Uptime/Expires     Ver   DR
Address                                                       Priority/Mode
fe80::201:7aff:fe62:bb7e gigabitethernet0/0/0        00:04:01/00:01:29  v2    1 / DR
fe80::201:7aff:fec0:525a gigabitethernet0/0/1        00:04:03/00:01:39  v2    1 / DR
```

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

**Step 5:** Enable MLD on gigabitethernet0/0/2 of Device3.

#Configure Device3.

Enable MLD on gigabitethernet0/0/2 of Device3.

```
Device3(config)#interface gigabitethernet0/0/2
Device3(config-if-gigabitethernet0/0/2)#ipv6 mld enable
Device3(config-if-gigabitethernet0/0/2)#exit
```

#View the MLD information of Device3 interface gigabitethernet0/0/2.

```
Device3#show ipv6 mld interface gigabitethernet0/0/2
Interface gigabitethernet0/0/2 (Index 11)
 MLD Enabled, Active
 Querier: fe80::201:7aff:fe5e:6d2f (Self)
 Default version: 2
 Querier parameter:
   Query interval is 125 seconds
   Querier timeout is 255 seconds
   Query response time is 10 seconds
   Last member query response interval is 1 seconds
   Last member query count is 2
   Group Membership interval is 260 seconds
   Robustness variable is 2
```

**Note:**

- You can configure the MLD version running on the interface via ipv6 mld version.

**Step 6:** Configure IPv6 PIM-SSM on all devices; the multicast group range of the SSM service is FF3X::/32.

#Configure Device1.

```
Device1(config)#ipv6 pim ssm default
```

#Configure Device2.

```
Device2(config)#ipv6 pim ssm default
```

#Configure Device3.

```
Device3(config)#ipv6 pim ssm defaul
```

**Step 7:** Check the result.

#PC sends the MLDv2 member relation report of the specified source group to add to multicast group FF30::1; the specified multicast source is 2001:1::1.

#Multicast Server sends the multicast packets with multicast group FF30::1.

#View the multicast member table of Device3.

```
Device3#show ipv6 mld groups detail
MLD Connected Group Membership
Total 1 Connected Groups
Group        Interface        Uptime    Expires    V1-Expires Last Reporter
ff30::1      gigabitethernet0/0/2                  00:26:42   not used   not used
fe80::210:94ff:fe00:1
 Group mode : Include
 TIB-A Count: 1
 TIB-B Count: 0


 TIB-A
 Source list: (R - Remote, M - SSM Mapping)
 Source                        Uptime    Expires  Flags
 2001:1::1                     00:05:55  00:03:41 R
```

#View the multicast route table of Device3.

```
Device3#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 VRF Name: Default
Total 0 (*,*,RP) entry
```

```
Total 0 (*,G) entry
Total 1 (S,G) entry
Total 0 (S,G,rpt) entry
Total 0 FCR entry
Up timer/Expiry timer


(2001:1::1, ff30::1)
Up time: 00:06:48
KAT time: 00:02:30
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: gigabitethernet0/0/0
SPT bit: TRUE
Flags:
 JOIN DESIRED
Upstream State: JOINED
 Local interface list:
  gigabitethernet0/0/2
 Joined interface list:
 Asserted interface list:
 Outgoing interface list:
  gigabitethernet0/0/2
 Packet count 275560
```

#PC can only receive the multicast service packet with multicast group FF30::1 sent by Source.

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.
- The default multicast group range of IPv6 PIM-SSM is FF3X::/32. You can modify the multicast group range of the IPv6 PIM-SSM service via the command ipv6 pim ssm range.
- For the multicast group G meeting the SSM condition, the multicast route table does not generate the (*,G) entry, but just generate the (S,G) entry.

## 12.3.3. Configure PIM-SMv6 Multicast Forwarding Control

### Network Requirements

- The whole network runs the PIM-SMv6 protocol.
- Receiver is one receiver of Device3 stub network.
- Device2 is C-BSR and C-RP.
- On Device2 and Device3, control for the multicast source, making PC only receive the multicast service packet sent by Multicast Server 1.

- Run MLDv2 between Device3 and the stub network.

## Network Topology

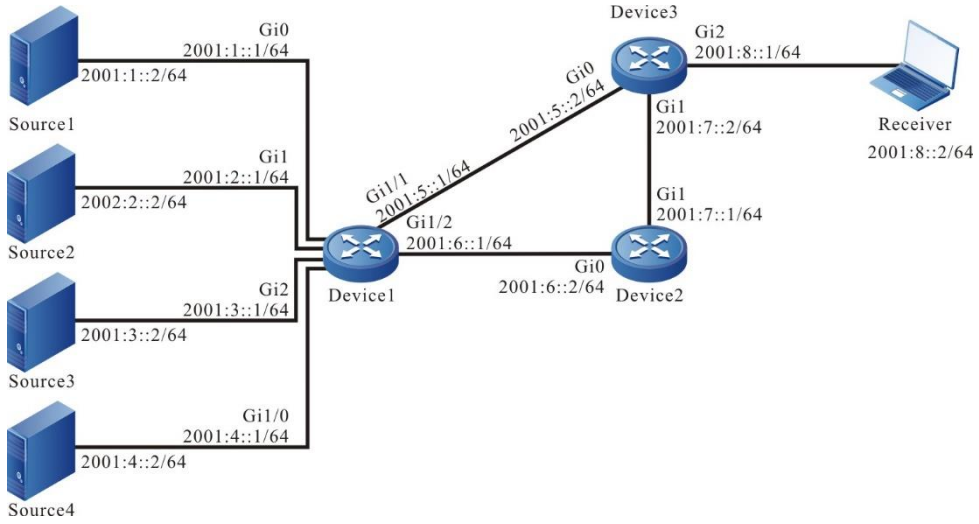


Figure 12-3 Networking of configuring PIM-SMv6 multicast forwarding control

## Configuration Steps

**Step 1:** Configure the IPv6 address of the interface. (omitted)

**Step 2:** Enable the unicast route protocol OSPFv3 so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface gigabitethernet0/0/0
Device1(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/0)#exit
Device1(config)#interface gigabitethernet0/0/1
Device1(config-if-gigabitethernet0/0/1)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/1)#exit
Device1(config)#interface gigabitethernet0/0/2
Device1(config-if-gigabitethernet0/0/2)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/2)#exit
Device1(config)#interface gigabitethernet0/0/3
Device1(config-if-gigabitethernet0/0/3)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/3)#exit
Device1(config)#interface gigabitethernet0/0/4
Device1(config-if-gigabitethernet0/0/4)#ipv6 router ospf 100 area 0
```

```
Device1(config-if-gigabitethernet0/0/4)#exit
Device1(config)#interface gigabitethernet0/0/5
Device1(config-if-gigabitethernet0/0/5)#ipv6 router ospf 100 area 0
Device1(config-if-gigabitethernet0/0/5)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface gigabitethernet0/0/0
Device2(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
Device2(config-if-gigabitethernet0/0/0)#exit
Device2(config)#interface gigabitethernet0/0/1
Device2(config-if-gigabitethernet0/0/1)#ipv6 router ospf 100 area 0
Device2(config-if-gigabitethernet0/0/1)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface gigabitethernet0/0/0
Device3(config-if-gigabitethernet0/0/0)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/0)#exit
Device3(config)#interface gigabitethernet0/0/1
Device3(config-if-gigabitethernet0/0/1)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/1)#exit
Device3(config)#interface gigabitethernet0/0/2
Device3(config-if-gigabitethernet0/0/2)#ipv6 router ospf 100 area 0
Device3(config-if-gigabitethernet0/0/2)#exit
```

#View the route table of Device3.

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L   ::1/128 [0/0]
    via ::, 3w2d:05:13:23, lo0
O   2001:1::/64 [110/2]
    via fe80::201:7aff:fe62:bb7e, 00:00:24, gigabitethernet0/0/0
O   2001:2::/64 [110/2]
    via fe80::201:7aff:fe62:bb7e, 00:00:24, gigabitethernet0/0/0
O   2001:3::/64 [110/2]
    via fe80::201:7aff:fe62:bb7e, 00:00:24, gigabitethernet0/0/0
O   2001:4::/64 [110/2]
    via fe80::201:7aff:fe62:bb7e, 00:00:24, gigabitethernet0/0/0
C   2001:5::/64 [0/0]
    via ::, 00:01:52, gigabitethernet0/0/0
L   2001:5::2/128 [0/0]
    via ::, 00:01:50, lo0
O   2001:6::/64 [110/2]
    via fe80::201:7aff:fe62:bb7e, 00:00:24, gigabitethernet0/0/0
          [110/2]
    via fe80::201:7aff:fec0:525a, 00:00:24, gigabitethernet0/0/1
C   2001:7::/64 [0/0]
    via ::, 00:01:25, gigabitethernet0/0/1
L   2001:7::2/128 [0/0]
    via ::, 00:01:24, lo0
C   2001:8::/64 [0/0]
    via ::, 00:01:16, gigabitethernet0/0/2
L   2001:8::1/128 [0/0]
    via ::, 00:01:14, lo0
```

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

**Step 3:** Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the interface.

#Configure Device1.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the related interfaces.

```
Device1(config)#ipv6 multicast-routing
```

```
Device1(config)#interface gigabitethernet0/0/0
Device1(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/0)#exit
Device1(config)#interface gigabitethernet0/0/1
Device1(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/1)#exit
Device1(config)#interface gigabitethernet0/0/2
Device1(config-if-gigabitethernet0/0/2)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/2)#exit
Device1(config)#interface gigabitethernet0/0/3
Device1(config-if-gigabitethernet0/0/3)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/3)#exit
Device1(config)#interface gigabitethernet0/0/4
Device1(config-if-gigabitethernet0/0/4)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/4)#exit
Device1(config)#interface gigabitethernet0/0/5
Device1(config-if-gigabitethernet0/0/5)#ipv6 pim sparse-mode
Device1(config-if-gigabitethernet0/0/5)#exit
```

#Configure Device2.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the related interfaces.

```
Device2(config)#ipv6 multicast-routing
Device2(config)#interface gigabitethernet0/0/0
Device2(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device2(config-if-gigabitethernet0/0/0)#exit
Device2(config)#interface gigabitethernet0/0/1
Device2(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
Device2(config-if-gigabitethernet0/0/1)#exit
```

#Configure Device3.

Globally enable the IPv6 multicast forwarding and enable the multicast protocol PIM-SMv6 on the related interfaces.

```
Device3(config)#ipv6 multicast-routing
Device3(config)#interface gigabitethernet0/0/0
Device3(config-if-gigabitethernet0/0/0)#ipv6 pim sparse-mode
Device3(config-if-gigabitethernet0/0/0)#exit
Device3(config)#interface gigabitethernet0/0/1
Device3(config-if-gigabitethernet0/0/1)#ipv6 pim sparse-mode
```

```
Device3(config-if-gigabitethernet0/0/1)#exit
Device3(config)#interface gigabitethernet0/0/2
Device3(config-if-gigabitethernet0/0/2)#ipv6 pim sparse-mode
Device3(config-if-gigabitethernet0/0/2)#exit
```

#View the information of the interface enabled with the PIM-SMv6 protocol on Device3 and the PIM-SMv6 neighbor information.

```
Device3#show ipv6 pim interface
PIM6 Interface Table:
PIM6 VRF Name: Default
Total 4 Interface entries
Total 0 External Interface entry
Total 0 Sparse-Dense Mode Interface entry

Interface      VIF   Ver/  VIF  Nbr   DR   BSR   CISCO   Neighbor
               Index  Mode  Flag  Count  Pri  Border Neighbor Filter
register_vif0   2     v2/S  UP
Address : fe80::201:7aff:fe5e:6d2d   Global Address: ::

gigabitethernet0/0/0        1     v2/S  UP   1    1    FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2d      Global Address: 2001:5::2              DR:
fe80::201:7aff:fe62:bb7e

gigabitethernet0/0/1        4     v2/S  UP   1    1    FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2e      Global Address: 2001:7::2              DR:
fe80::201:7aff:fec0:525a

gigabitethernet0/0/2        3     v2/S  UP   0    1    FALSE  FALSE
Address : fe80::201:7aff:fe5e:6d2f      Global Address: 2001:8::1              DR:
fe80::201:7aff:fe5e:6d2f
Device3#show ipv6 pim neighbor
PIM6 Neighbor Table:
PIM6 VRF Name: Default
Total 2 Neighbor entries

Neighbor            Interface      Uptime/Expires     Ver   DR
Address                                               Priority/Mode
fe80::201:7aff:fe62:bb7e gigabitethernet0/0/0        00:07:08/00:01:25   v2    1 / DR
```

```
fe80::201:7aff:fec0:525a gigabitethernet0/0/1          00:00:18/00:01:27   v2    1 / DR
```

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

**Step 4:** Configure gigabitethernet0/0/0 of Device2 as the C-BSR and C-RP of the whole network and the multicast group range of the C-RP service is FF00::/8.

#Configure Device2.

```
Device2(config)#ipv6 pim bsr-candidate gigabitethernet0/0/0
Device2(config)#ipv6 pim rp-candidate gigabitethernet0/0/0
```

#View the BSR and RP information of Device3.

```
Device3#show ipv6 pim bsr-router
PIM6v2 Bootstrap information
PIM6 VRF Name: Default
  BSR address: 2001:6::2
  BSR Priority: 0
  Hash mask length: 126
  Up time: 00:00:21
  Expiry time: 00:01:54
  Role: Non-candidate BSR
State: Accept Preferred

Device3#show ipv6 pim rp mapping
PIM6 Group-to-RP Mappings Table:
PIM6 VRF Name: Default
Total 1 RP set entry
Total 1 RP entry

  Group(s): ff00::/8
  RP count: 1
    RP: 2001:6::2
      Info source: 2001:6::2, via bootstrap, priority 192
      Up time: 00:00:28
      Expiry time: 00:02:02
```

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

**Step 5:** On Device2 and Device3, control for the multicast source, making PC only receive the multicast service packet sent by Multicast Server 1.

#On Device2, configure the accepted register message access list, filtering the register message of Multicast Server 4.

```
Device2(config)#ipv6 access-list extended 7001
Device2(config-std-nacl)#deny ipv6 host 2001:4::2 any
Device2(config-std-nacl)#permit ipv6 any any
Device2(config-std-nacl)#exit
Device2(config)#ipv6 pim accept-register list 7001
```

#On interface valn6 and gigabitethernet0/0/0 of Device3, configure the ingress IPv6 acl, filtering the multicast service packets of Multicast Server 3.

```
Device3(config)#ipv6 access-list extended 7001
Device3(config-v6-list)#deny ipv6 host 2001:3::2 any
Device3(config-v6-list)#permit ipv6 any any
Device3(config-v6-list)#exit
Device3(config)#interface gigabitethernet0/0/0
Device3(config-if-gigabitethernet0/0/0)#ipv6 access-group 7001 in
Device3(config-if-gigabitethernet0/0/0)#exit
Device3(config)#interface gigabitethernet0/0/1
Device3(config-if-gigabitethernet0/0/1)#ipv6 access-group 7001 in
Device3(config-if-gigabitethernet0/0/1)#exit
```

#On interface gigabitethernet0/0/2 of Device3, configure the ingress IPv6 acl, filtering the multicast service packets of Multicast Server 2.

```
Device3(config)#ipv6 access-list extended 7002
Device3(config-v6-list)#deny ipv6 host 2001:2::2 any
Device3(config-v6-list)#permit ipv6 any any
Device3(config-v6-list)#exit
Device3(config)#interface gigabitethernet0/0/2
Device3(config-if-gigabitethernet0/0/2)#ipv6 access-group 7002 out
Device3(config-if-gigabitethernet0/0/2)#exit
```

**Step 7:** Check the result.

#PC sends the MLDv2 member relation report to add to multicast group FF10::1.

# Multicast Server 1, Multicast Server 2, Multicast Server 3, and Multicast Server 4 all send the multicast packets of multicast group FF10::1.

#View the multicast member table of Device3.

```
Device3#show ipv6 mld groups
MLD Connected Group Membership
Total 1 Connected Groups
Group    Interface          Uptime    Expires   V1-Expires  Last Reporter
ff10::1  gigabitethernet0/0/2          00:35:31  00:03:31 not used    fe80::210:94ff:fe00:1
```

#View the multicast route table of Device3.

```
Device3#show ipv6 pim mroute
IP Multicast Routing Table:
PIM6 VRF Name: Default
Total 0 (*,*,RP) entry
Total 1 (*,G) entry
Total 2 (S,G) entries
Total 2 (S,G,rpt) entries
Total 0 FCR entry
Up timer/Expiry timer


(*, ff10::1)
Up time: 00:04:25
RP: 2001:6::2
RPF nbr: fe80::201:7aff:fec0:525a
RPF idx: gigabitethernet0/0/1
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
    gigabitethernet0/0/2
  Joined interface list:
  Asserted interface list:


(2001:1::2, ff10::1)
Up time: 00:03:33
KAT time: 00:01:51
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: gigabitethernet0/0/0
SPT bit: TRUE
```

```
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    vlan9
  Packet count 159075

(2001:1::2, ff10::1, rpt)
Up time: 00:03:33
RP: 2001:6::2
Flags:
  RPT JOIN DESIRED
  PRUNE DESIRED
  RPF SGRPT XG EQUAL
Upstream State: PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    gigabitethernet0/0/2

(2001:2::2, ff10::1)
Up time: 00:03:33
KAT time: 00:01:51
RPF nbr: fe80::201:7aff:fe62:bb7e
RPF idx: gigabitethernet0/0/0
SPT bit: TRUE
Flags:
  JOIN DESIRED
Upstream State: JOINED
  Local interface list:
  Joined interface list:
  Asserted interface list:
  Outgoing interface list:
    gigabitethernet0/0/2
```

```
  Packet count 156062

(2001:2::2, ff10::1, rpt)
Up time: 00:03:33
RP: 2001:6::2
Flags:
  RPT JOIN DESIRED
  PRUNE DESIRED
  RPF SGRPT XG EQUAL
Upstream State: PRUNED
  Local interface list:
  Pruned interface list:
  Outgoing interface list:
    gigabitethernet0/0/2
```

**Note:**

- The viewing method of Device1 and device2 is the same as that of Device3, so the viewing process is omitted.

#View the matching of IPv6 ACL on Device2.

```
Device2#show ipv6 access-list 7001
ipv6 access-list extended 7001
 10 deny ipv6 host 2001:4::2 any     14 matches
 20 permit ipv6 any any     51 matches
```

#View the matching of IPv6 ACL on Device3.

```
Device3#show ipv6 access-list 7001
ipv6 access-list extended 7001
 10 deny ipv6 host 2001:3::2 any     10760 matches
 20 permit ipv6 any any     4089685 matches

Device3#show ipv6 access-list 7002
ipv6 access-list extended 7002
 10 deny ipv6 host 2001:2::2 any     2046914 matches
 20 permit ipv6 any any     2049595 matches
```

#PC end can only receive the multicast service packets sent by Multicast Server 1.

**Caution:**

- When performing the multicast source control, you'd better first configure the multicast source control and then on-demand multicast source, because by default, after receiving the multicast service packet, the receiving end DR performs the SPT switching. If first on-demanding multicast source and then performing the multicast forwarding control,

the multicast forwarding control does not take function. To prevent the multicast forwarding control from not taking function, you can configure not permitting SPT switching on the receiving end DR.

# 13. ОБЩАЯ ИНФОРМАЦИЯ

## 13.1. Замечания и предложения

Мы всегда стремимся улучшить нашу документацию и помочь вам работать лучше, поэтому мы хотим услышать вас. Мы всегда рады обратной связи, в особенности:

- ошибки в содержании, непонятные или противоречащие места в тексте;
- идеи по улучшению документации, чтобы находить информацию быстрее;
- неработающие ссылки и замечания к навигации по документу.

Если вы хотите написать нам по поводу данного документа, то используйте, пожалуйста, форму обратной связи на qtech.ru.

## 13.2. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» −> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» −> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

## 13.3. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться нашей автоматизированной системой запросов технического сервис-центра helpdesk.qtech.ru.

Телефон Технической поддержки +7 (495) 797-33-11 доб. 0