

Multicast Configuration

Оглавление

1.	CONFIGURING IP MULTICASTING	1
1.1	Overview	1
1.2	Applications	1
1.2.1	PIM DM Applications	1
1.2.2	PIM SM Applications	2
1.3	Features	3
1.3.1	Configuring Basic Functions of IP Multicasting	5
1.3.2	Configuring a TTL Threshold	5
1.3.3	Configuring the Number of Entries That Can Be Added to the Multicast Routing Table	6
1.3.4	Configuring an IP Multicasting Border	6
1.3.5	Configuring an IP Multicasting Static Route	7
1.3.6	Configuring Layer 2 Direction Control for Multicast Streams	7
1.3.7	Configuring RPF Route Selection Based on the Longest Match Rule	7
1.3.8	Configuring Multicast Non Stop Forwarding Parameters	8
1.3.9	Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries	9
1.4	Configuration	9
1.4.1	Configuring Basic Functions of IP Multicasting	10
1.4.2	Configuring a TTL Threshold	14
1.4.3	Configuring the Number of Entries That Can Be Added to the Multicast Routing Table	16
1.4.4	Configuring an IP Multicasting Border	19
1.4.5	Configuring an IP Multicasting Static Route	20
1.4.6	Configuring Layer 2 Direction Control for Multicast Streams	23
1.4.7	Configuring RPF Route Selection Based on the Longest Match Rule	24
1.4.8	Configuring Multicast Non Stop Forwarding Parameters	26
1.4.9	Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries	28
1.5	Monitoring	29

2.	CONFIGURING IPV6 MULTICAST	32
2.1	Overview	32
2.2	Applications	32
2.2.1	Typical Application of PIM SMv6	32
2.3	Features	33
2.3.1	Configuring IPv6 Multicast Basic Functions	35
2.3.2	Configuring the Number of Entries That Can Be Added to the IPv6 Multicast Routing Table	35
2.3.3	Configuring the IPv6 Multicast Border	36
2.3.4	Configuring IPv6 Multicast Static Routing	36
2.3.5	Configuring Layer 2 Flow Direction Control for Multicast Streams	37
2.3.6	Configuring RPF Route Selection According to the Longest Matching Principle	37
2.4	Configuration	38
2.4.1	Configuring IPv6 Multicast Basic Functions	38
2.4.2	Configuring the Number of Entries That Can Be Added to the IPv6 Multicast Routing Table	41
2.4.3	Configuring the IPv6 Multicast Border	45
2.4.4	Configuring IPv6 Multicast Static Routing	47
2.4.5	Configuring Layer 2 Flow Direction Control for Multicast Streams	49
2.4.6	Configuring RPF Route Selection According to the Longest Matching Principle	50
2.5	Monitoring	53
3.	CONFIGURING IGMP	55
3.1	Overview	55
3.2	Applications	55
3.2.1	Local IGMP Service	55
3.2.2	IGMP Proxy Service	56
3.3	Features	57
3.3.1	IGMP Router	58
3.3.2	IGMP Querier	59
3.3.3	IGMP Group Filtering	59
3.3.4	Static IGMP Group	60
3.3.5	Simulating Hosts to Join IGMP Groups	60
3.3.6	IGMP Proxy	61
3.3.7	IGMP SSM Mapping	61
3.4	Configuration	62

3.4.1	Configuring IGMP Basic Functions	62
3.4.2	Configuring IGMP Routers	64
3.4.3	Configuring IGMP Querier	68
3.4.4	Configuring IGMP Group Filtering	70
3.4.5	Configuring IGMP Proxy	73
3.4.6	Configuring IGMP SSM Mapping	75
3.5	Monitoring	76
4.	CONFIGURING MLD	79
4.1	Overview	79
4.2	Applications	79
4.2.1	Configuring the MLD Service on the Local Network	79
4.2.2	Configuring the MLD Proxy Service	80
4.3	Features	81
4.3.1	Setting MLD Router Parameters	82
4.3.2	Querier Selection Process or Timeout Mechanism	83
4.3.3	Filtering MLD Groups	83
4.3.4	Supporting Static MLD Groups	84
4.3.5	Configuring Simulated Host Group Information	84
4.3.6	Supporting MLD Proxy	85
4.3.7	Supporting SSM MAP	85
4.4	Configuration	86
1.1.1		86
1.1.1		86
1.1.1		86
1.1.1		86
4.4.1	Configuring Basic Functions of MLD	87
4.4.2	Configuring MLD Router Parameters	88
4.4.3	Querier Selection Process or Timeout Mechanism	92
4.4.4	Filtering MLD Groups	94
4.4.5	MLD Proxy	97
4.4.6	Supporting SSM MAP	99
4.5	Monitoring	101

5.	CONFIGURING PIM-DM	103
5.1	Overview	103
5.2	Applications	103
5.2.1	Providing the Multicast Service in the Same Network	103
1.1.1	PIM-DM Application in a Hot Backup Environment	104
5.3	Features	105
5.3.1	PIM DM Neighbor	106
5.3.2	PIM DM MDT	108
5.3.3	PIM DM SRM	108
5.3.4	MIB	109
5.4	Configuration	109
5.4.1	Configuring PIM DM Basic Functions	110
5.4.2	Configuring PIM DM Neighbors	113
5.4.3	Configuring PIM DM SRMs	117
5.4.4	Configuring PIM DM MIB	120
5.5	Monitoring	121
6.	CONFIGURING PIM-SM	122
6.1	Overview	122
6.2	Applications	122
6.2.1	Enabling ASM for PIM SM	122
6.2.2	Enabling SSM for PIM SM	123
1.1.2	PIM-SM Application in a Hot Backup Environment	124
6.3	Features	125
6.3.1	PIM SM Neighbor	127
6.3.2	DR Election	128
6.3.3	BSR Mechanism	129
6.3.4	RP Mechanism	130
6.3.5	Register Information of the Multicast Source	132
6.3.6	Creating an RPT	134
6.3.7	Creating an SPT	135
6.3.8	ASM and SSM	136
6.4	Configuration	137
6.4.1	Configuring Basic PIM SM Functions	139

6.4.2	Configuring PIM SM Neighbors	152
6.4.3	Configuring BSR Parameters	156
6.4.4	Configuring RP and DR Parameters	162
6.4.5	Configuring the Interval for Sending a Join/Prune Packet	180
6.4.6	Configuring the Router of Last Hop to Switch from an RPT to SPT	183
6.5	Monitoring	186
7.	CONFIGURING PIM-SMv6	188
7.1	Overview	188
7.2	Applications	188
7.2.1	ASM Implementation by Using PIM SMv6	188
7.2.2	SSM Implementation by Using PIM SMv6	189
7.2.3	Application Example of an Embedded RP	190
7.2.4	PIM SMv6 Application in a Hot Backup Environment	191
7.3	Features	192
7.3.1	Establishment of PIM Neighbor Relationships	194
7.3.2	DR Election	195
7.3.3	BSR Mechanism	196
7.3.4	RP Mechanism	198
7.3.5	Registration Information About a Multicast Source	199
7.3.6	RPT Establishment	202
7.3.7	SPT Establishment	202
7.3.8	ASM and SSM Models	203
7.4	Configuration	204
7.4.1	Configuring Basic Functions of PIM SMv6	204
7.4.2	Configuring PIM Neighbor Parameters	215
7.4.3	Configuring BSR Parameters	220
7.4.4	Configuring RP and DR Parameters	227
7.4.5	Configuring the Transmission Interval of Join/Prune Packets	242
7.4.6	Configuring the Last Hop Device to Switch from the RPT to the SPT	245
7.5	Monitoring	246
8.	CONFIGURING MSDP	248
8.1	Overview	248
8.2	Applications	248

8.2.1	Cross Domain Multicast	248
8.2.2	Anycast RP	249
8.3	Features	250
8.3.1	Establishing an MSDP Peer Relationship	250
8.3.2	Receiving and Forwarding SA Messages	251
8.4	Configuration	254
8.4.1	Configuring Cross Domain Multicast	255
8.4.2	Configuring an Anycast RP	261
8.4.3	Configuring the Peer RPF Check Green Channel	266
8.4.4	Enabling Security Measures	270
8.4.5	Restricting Broadcasting of SA Messages	273
8.4.6	Managing MSDP Peers	278
8.4.7	Modifying Protocol Parameters	280
8.5	Monitoring	283
9.	CONFIGURING IGMP SNOOPING	285
9.1	Overview	285
9.2	Applications	286
9.2.1	Layer 2 Multicast Control	286
9.2.2	Shared Multicast Services (Multicast VLAN)	287
9.2.3	Premium Channels and Preview	287
9.3	Features	288
9.3.1	Listening to IGMP Packets	290
9.3.2	IGMP Snooping Working Modes	292
9.3.3	IGMP Security Control	294
9.3.4	IGMP Profile	296
9.3.5	IGMP QinQ	297
9.3.6	IGMP Querier	298
9.4	Configuration	300
9.4.1	Configuring Basic IGMP Snooping Functions (IVGL Mode)	303
9.4.2	Configuring Basic IGMP Snooping Functions (SVGL Mode)	307
9.4.3	Configuring Basic IGMP Snooping Functions (IVGL SVGL Mode)	311
9.4.4	Configuring the Packet Processing	315
9.4.5	Configuring IGMP Security Control	324

9.4.6	Configuring an IGMP Profile	336
9.4.7	Configuring IGMP QinQ	338
9.4.8	Configuring an IGMP Querier	339
9.5	Monitoring	344
10.	CONFIGURING MLD SNOOPING	346
10.1	Overview	346
10.1.1	Two Types of MLD Snooping Ports	346
10.1.2	Work Mode of MLD Snooping	347
10.1.3	Working Principle of MLD Snooping	347
10.1.4	Source Port Check	348
10.2	Applications	349
10.2.1	MLD Snooping SVGL Trans VLAN Multicast On demand	349
10.2.2	Source Port Filtering	350
10.3	Features	350
10.3.1	Globally Enabling MLD Snooping	352
10.3.2	VLAN based MLD Snooping	352
10.3.3	Aging Time of Multicast Router Ports	352
10.3.4	Dynamic Multicast Router Port Learning	352
10.3.5	Aging Time of Dynamic Member Ports	353
10.3.6	Fast Leave of Multicast Group Member Ports	353
10.3.7	MLD Report Packet Suppression	353
10.3.8	Source Port Check	353
10.3.9	Port based Specific Multicast Group Filtering	353
10.3.10	Maximum Number of Multicast Groups Supported by a Port	353
10.4	Configuration	353
10.4.1	Configuring Basic Functions of MLD Snooping	354
10.5	Monitoring	359

1. CONFIGURING IP MULTICASTING

1.1 Overview

IP multicasting is abstracted hardware multicasting and an extended multicast routing protocol on the standard IP network layer.

In traditional IP transmission, only one host can send packets to a single host (unicast communication) or all hosts (broadcast communication). However, the multicast technology provides the third choice: a host can send packets to certain specified hosts.

IP multicasting is applicable to one-to-many multimedia applications.

1.2 Applications

Application	Description
PIM-DM Applications	The PIM-DM multicast service is provided on the same network.
PIM-SM Applications	The PIM-SM multicast service is provided on the same network.

1.2.1 PIM-DM Applications

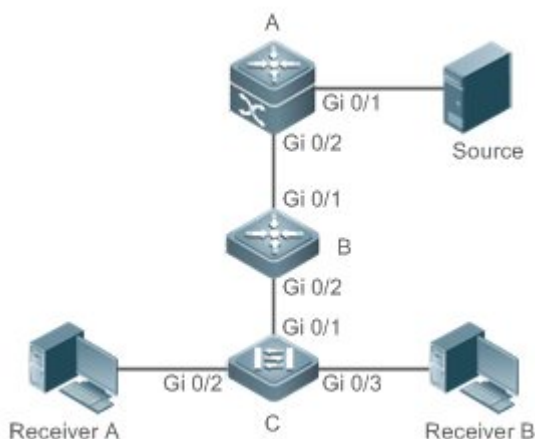
Scenario

The PIM-DM multicast service is provided on the same network.

As shown in Figure 1-1:

- A multicast source sends a multicast packet, and receiver A and receiver B on the same network receive the multicast packet.

Figure 1-1



Remark	A and B are layer-3 devices and C is a layer-2 access device.
s	Source is connected to the Gi 0/1 interface of A, and receiver A and receiver B are connected to the Gi 0/2 and Gi 0/3 interfaces of C.

Deployment

- Run the Open Shortest Path First (OSPF) protocol on the same network to implement unicast routing.
- Run PIM-DM on the same network to implement multicast routing.
- Run the Internet Group Membership Protocol (IGMP) in a user host network segment to implement group member management.

1.2.2 PIM-SM Applications

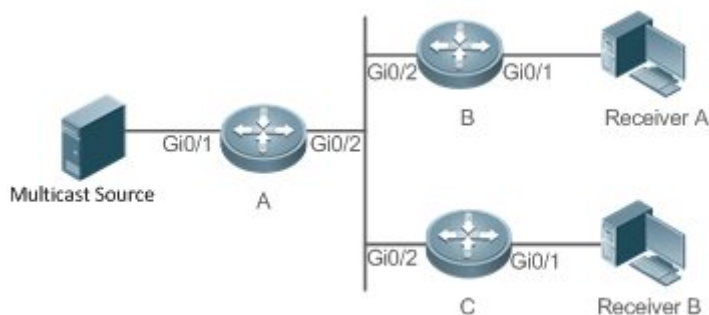
Scenario

The PIM-SM multicast service is provided on the same network.

As shown in Figure 1-2:

- A multicast source sends a multicast packet, and receiver A and receiver B on the same network receive the multicast packet.

Figure 1-2



Remark	A, B, and C are layer-3 routers.
s	The multicast source is connected to the Gi 0/1 interface of A, receiver B is connected to the Gi 0/1 interface of B, and receiver B is connected to the Gi 0/1 interface of C.

Deployment

- Run OSPF on the same network to implement unicast routing.
- Run PIM-SM on the same network to implement multicast routing.
- Run IGMP in a user host network segment to implement group member management.

1.3 Features

Basic Concepts

❖ PIM Routers and PIM Interfaces

Routers enabled with PIM are called PIM routers. Interfaces enabled with PIM protocol are called PIM interfaces.

Multicast packets are forwarded on PIM routers. The PIM interfaces for receiving multicast packets are called upstream interfaces, and the PIM interfaces for sending multicast packets are called downstream interfaces.

The network segments where upstream interfaces are located are called upstream network segments. The network segments where downstream interfaces are located are called downstream network segments.

❖ PIM Network and PIM Domain

PIM routers are connected through PIM interfaces and form a PIM network.

On certain PIM interfaces, borders are configured to divide a large PIM network into multiple PIM domains. Borders may reject specified multicast packets or limit transmission of PIM messages.

❖ Multicast Distribution Tree, DR and RP

Multicast packets are transmitted from one point to multiple points. The forwarding path is in a tree structure. This forwarding path is called a multicast distribution tree (MDT) and has the following types:

- Rendezvous Point Tree (RPT): The RP is regarded as the root and the designated router (DR) that connects group members is regarded as a leaf.
- Shortest Path Tree (SPT): The DR that connects multicast sources is regarded as the root, and RP or DR that connects group members is regarded as a leaf.

The DR and RP are functional roles for a PIM router.

- The RP collects multicast sources and group member information on the network.
- The DR that connects multicast sources reports multicast source information to the RP. The DR that connects group members reports group member information to the RP.

❖ (*,G) and (S,G)

- (*,G): Packets sent from any source to group G, routing entries corresponding to the packets, and forwarding path (RPT) corresponding to the packets.
- (S,G): Packets sent from source S to group G, routing entries corresponding to the packets, and forwarding path (SPT) corresponding to the packets.

❖ ASM and SSM

PIM-SM supports the following multicast models that are applicable to different multicast address segments:

- Any-Source Multicast (ASM): In the ASM model, user hosts cannot select multicast sources. User hosts join a group and receive packets sent from all sources to the group.
 - Source-Specific Multicast (SSM): In the SSM model, user hosts can select multicast sources. User hosts specify source addresses when joining a group and receive only packets sent from specified sources to the group.
-
- SSM model requirements: User hosts must know the multicast source address in advance using other network services so that the hosts can select multicast sources.

Overview

Feature	Description
Configuring Basic Functions of IP Multicasting	Creates a PIM network and provides data sources and user terminals on the network with the IPv4 multicast service.
Configuring a TTL Threshold	Configures a TTL threshold for an interface, that is, the minimum TTL value of multicast packets allowed on an interface.
Configuring the Number of Entries That Can Be Added to the Multicast Routing Table	Limits the number of entries that can be added to the multicast routing table.
Configuring an IP Multicasting Border	Configures an interface as a multicast border for a specified group.
Configuring an IP Multicasting Static Route	Allows the multicast forwarding path to be different from the unicast path.
Configuring Layer-2 Direction Control for Multicast Streams	Allows a specified multicast stream to be configured with multiple commands, that is, to be configured with multiple ports that can forward the stream. Once direction control is configured for a multicast stream, the stream can be forwarded only by these configured interfaces. Other interfaces are not permitted to forward the stream.
Configuring RPF Route Selection Based on the Longest Match Rule	Selects an optimal route respectively from the multicast static routing table, MBGP routing table, and unicast routing table according to RPF rules. Among these three routes, the one with the longest match mask is selected as the RPF route.

Feature	Description
Configuring Multicast Non-Stop Forwarding Parameters	During normal running, SSP synchronizes the hardware multicast forwarding table to the management board in real time. After the management board is switched, the command for configuring the multicast control plane of the original slave management board is loaded, and the multicast protocol (such as PIM-SM or IGMP Snooping) re-converges. The multicast non-stop forwarding function ensures continuous forwarding of multicast data streams during re-convergence of the multicast protocol.
Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries	Deletes the earliest hardware entries and adds new entries if the hardware forwarding table overflows when you create multicast forwarding entries.

1.3.1 Configuring Basic Functions of IP Multicasting

Create a PIM network and provide data sources and user terminals on the network with the IPv4 multicast service.

Working Principle

A device maintains the routing table for forwarding multicast packets through multicast routing protocols (such as PIM-DM or PIM-SM) and learns the states of group members in the directly connected network segment through IGMP. A host sends IGMP Report messages to join a specified IGMP group.

Related Configuration

❖ Enabling IPv4 Multicast Routing

By default, IPv4 multicast routing is disabled.

Run **ip multicast-routing** to enable IPv4 multicast routing.

❖ Configuring IP Multicasting on an Interface

By default, IP multicasting is disabled on an interface.

Run **ip pim sparse-mode** or **ip pim dense-mode** to enable IP multicasting on an interface.

1.3.2 Configuring a TTL Threshold

Configure a TTL threshold for an interface, that is, the minimum TTL value of multicast packets allowed on an interface.

Working Principle

Configure a TTL threshold for an interface and check the TTL values of multicast packets. Multicast packets whose TTL values are larger than the TTL threshold of the interface are forwarded and those whose TTL values are smaller are discarded.

Related Configuration

❖ Configuring a TTL Threshold

By default, the TTL threshold of an interface is 0.

Run **ip multicast ttl-threshold *ttl-value*** to change the TTL threshold of an interface. The value ranges from 0 to 255.

A larger value of *ttl-value* means a larger TTL value of multicast packets to be forwarded.

1.3.3 Configuring the Number of Entries That Can Be Added to the Multicast Routing Table

Each multicast data packet received on the device maintains a corresponding IP multicast route forwarding entry. However, excess multicast routing entries may exhaust device memory and deteriorate device performance. You can limit the number of entries in the IP multicast routing table based on the actual network and service performance requirements.

Working Principle

The number of entries in the IP multicasting routing table is limited based on the actual network and service performance requirements to ensure device performance.

Related Configuration

❖ Configuring the Number of Entries That Can Be Added to the Multicast Routing Table

By default, a maximum of 1024 entries can be added to an IP multicast routing table.

Run **ip multicast route-limit *limit* [*threshold*]** to change the number of entries that can be added to the IP multicasting routing table. The value ranges from 1 to 65536.

A larger value of *limit* means a larger number of entries that can be added to the IP multicasting routing table.

1.3.4 Configuring an IP Multicasting Border

Configure an IP multicasting border to specify the transmission range of multicast packets.

Working Principle

An IP multicasting border is configured to specify the transmission range of multicast packets. When an IP multicasting border is configured on an interface, this interface cannot forward or receive multicast packets, including those sent from the local host.

Related Configuration

❖ Configuring an IP Multicasting Border

By default, no IP multicasting border is configured.

Run **ip multicast boundary** *access-list* [**in** | **out**] to configure an IP multicasting border.

1.3.5 Configuring an IP Multicasting Static Route

Configure an IP multicasting static route to specify an RPF interface or RPF neighbor for multicast packets from specified multicast sources.

Working Principle

An RPF check is performed once multicast packets are forwarded. An IP multicasting static route can be configured to specify an RPF interface or RPF neighbor for multicast packets from specified multicast sources.

Related Configuration

❖ Configuring an IP Multicasting Static Route

By default, no IP multicasting static route is configured.

Run **ip mroute** *source-address mask* { [**bgp** | **isis** | **ospf** | **rip** | **static**] { *v4rpf-addrress* | *interface-type interface-number* } } [*distance*] to configure an IP multicasting static route.

1.3.6 Configuring Layer-2 Direction Control for Multicast Streams

Configure layer-2 direction control for multicast streams to control the forwarding of multicast streams on an interface.

Working Principle

Configure layer-2 direction control for multicast streams and a forwarding interface so that multicast streams can be forwarded only through configured interfaces. In this case, layer-2 forwarding of multicast streams can be controlled.

Related Configuration

❖ Configuring Layer-2 Direction Control for Multicast Streams

By default, layer-2 direction control for multicast streams is disabled.

Run **ip multicast static** *source-address group-address interface-type interface-number* to configure layer-2 direction control for multicast streams.

1.3.7 Configuring RPF Route Selection Based on the Longest Match Rule

Select an optimal route respectively from the multicast static routing table, MBGP routing table, and unicast routing table and select the one with the longest match mask as the RPF route from the three optimal routes.

Working Principle

A multicast static route, an MBGP route, and a unicast route that can be used for RPF check are selected respectively from the multicast static routing table, MBGP routing table, and unicast routing table according to RPF rules.

- If the longest match rule is used, the route with the longest match mask is selected as the RPF route. If the three routes have the same mask, the one with the highest priority is selected as the RPF route. If they have the same priority, the RPF routes are selected in the sequence of multicast static route, MBGP route, and unicast route.
- Otherwise, the one with the highest priority is selected as the RPF route. If they have the same priority, the RPF routes are selected in the sequence of multicast static route, MBGP route, and unicast route.

Related Configuration

❖ Configuring RPF Route Selection Based on the Longest Match Rule

By default, the route with the highest priority is selected as the RPF route. If they have the same priority, the RPF routes are selected in the sequence of multicast static route, MBGP route, and unicast route.

Run **ip multicast rpf longest-match** to configure RPF route selection based on the longest match rule.

1.3.8 Configuring Multicast Non-Stop Forwarding Parameters

The non-stop forwarding function ensures continuous forwarding of multicast data streams during the re-convergence of multicast protocols.

Working Principle

During normal running, SSP synchronizes the hardware multicast forwarding table to the management board in real time. After the management board is switched, the command for configuring the multicast control plane of the original slave management board is loaded, and the multicast protocol (such as PIM-SM or IGMP Snooping) re-converges. The multicast non-stop forwarding function ensures continuous forwarding of multicast data streams during re-convergence of multicast protocols.

After the configured protocol convergence period times out, all multicast forwarding table entries that are not updated during the convergence period are deleted.

Related Configuration

❖ Configuring the Maximum Period for Multicast Protocol Convergence

By default, the maximum period for multicast protocol convergence is 20s.

Run **msf nsf convergence-time time** to configure the maximum period for multicast protocol convergence. The value ranges from 0 to 3600s.

A larger value of *time* means a longer maximum period for multicast protocol convergence.

❖ Configuring the Multicast Packet Leakage Period

By default, the multicast packet leakage period is 30s.

Run **msf nsf leak interval** to configure the multicast packet leakage period. The value ranges from 0 to 3600s.

A larger value of *interval* means a longer leakage period.

1.3.9 Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries

Delete the earliest hardware entries and adds new entries if the hardware forwarding table overflows when you create multicast forwarding entries.

Working Principle

Delete the earliest hardware entries and adds new entries if the hardware forwarding table overflows when you create multicast forwarding entries .

Related Configuration

❖ Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries

By default, the overwriting mechanism upon the overflow of multicast hardware forwarding entries is disabled.

Run **msf ipmc-overflow override** to configure the overwriting mechanism upon overflow of multicast hardware forwarding entries.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of IP Multicasting	(Mandatory) It is used to configure the multicast service.	
	ip multicast-routing	Enables the IPv4 multicast routing function.
Configuring a TTL Threshold	Optional.	
	ip multicast ttl-threshold <i>tvl-value</i>	Configures a TTL threshold for an interface.
Configuring the Number of Entries That Can Be Added to the Multicast Routing Table	ip multicast route-limit <i>limit</i> [<i>threshold</i>]	Limits the number of entries that can be added to the multicast routing table.

Configuring an IP Multicasting Border	ip multicast boundary <i>access-list</i> [in out]	Configures an interface as a multicast border for a specified group.
Configuring an IP Multicasting Static Route	ip mroute <i>source-address mask</i> { [bgp isis ospf rip static] { <i>v4rpf-address</i> <i>interface-type interface-number</i> } } [<i>distance</i>]	Configures an IP multicasting static route.
Configuring Layer-2 Direction Control for Multicast Streams	ip multicast static <i>source-address group-address interface-type interface-number</i>	Controls the direction of data streams on layer-2 interfaces.
Configuring RPF Route Selection Based on the Longest Match Rule	ip multicast rpf longest-match	Configures RPF route selection based on the longest match rule.
Configuring Multicast Non-Stop Forwarding Parameters	msf nsf convergence-time <i>time</i>	Configures the maximum period for multicast protocol convergence.
	msf nsf leak <i>time</i>	Configures the multicast packet leakage period.
Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries	msf ipmc-overflow override	Configures the overwriting mechanism upon overflow of multicast hardware forwarding entries.

1.4.1 Configuring Basic Functions of IP Multicasting

Configuration Effect

- Create a PIM network and provide data sources and user terminals on the network with the IPv4 multicast service.

Notes

- A PIM network needs to use existing unicast routes on the network. Therefore, IPv4 routes must be configured on the network.

Configuration Steps

- ❖ Enabling IPv4 Multicast Routing
 - Mandatory.
 - IPv4 multicast routing should be enabled on each router unless otherwise specified.
- ❖ Enabling IP Multicasting for an Interface
 - Mandatory.
 - IP multicasting protocol should be enabled on interfaces unless otherwise specified:

Verification

Enable multicast sources to send multicast packets and user hosts to join the groups.

- Check whether the user hosts can successfully receive packets from each group.

Related Commands

❖ Enabling IPv4 Multicast Routing

Command	<code>ip multicast-routing</code>
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	-

❖ Configuring IP Multicasting

- For IGMP configuration, see the IGMP section.
- For PIM-DM configuration, see the PIM-DM section.
- For PIM-SM configuration, see the PIM-SM section.

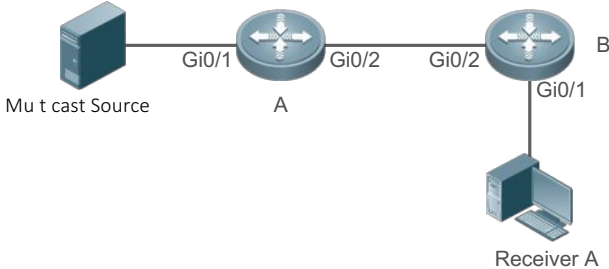
After layer-3 multicasting is enabled in the private VLAN and super VLAN and a multicast source exists in the sub-VLAN, an extra entry whose ingress is the sub-VLAN into which the multicast stream enters needs to be copied due to the validity check during multicast forwarding. This results in occupation of one more multicast hardware entry and one less in the multicast capacity.

❖ Displaying Information About the Multicast Forwarding Table

Command	<code>show ip mroute [group-or-source-address [group-or-source-address]] [dense sparse] [summary count]</code>
Parameter Description	<p><i>group-or-source-address</i>: Specifies a group address or source address.</p> <p><i>group-or-source-address</i>: Specifies a group address or source address.</p> <p>dense: Displays the core entry of PIM-DM multicast.</p> <p>sparse: Displays the core entry of PIM-SM multicast.</p> <p>summary: Displays summary information about multicast routing entries.</p> <p>count: Displays counting information about multicast routing entries.</p>
Command Mode	Privilege, global and interface configuration modes
Usage Guide	<p>The three parameters are optional, and the source address and group address must be specified simultaneously.</p> <p>When no source address or group address is specified, all MFC entries are displayed.</p> <p>When only the source address and group address are specified, MFC entries of the source address and group address are displayed.</p>

Configuration Example

❖ Creating the IP Multicast Service on the IPv4 Network and Supporting PIM-DM

<p>Scenario Figure 1-3</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure an IPv4 unicast routing protocol (such as OSPF) on a router. ➤ Enable IPv4 multicast routing on all routers. ➤ Enable PIM-DM on device interconnection interfaces and interfaces for connecting user hosts and multicast sources.
<p>A</p>	<pre>A# configure terminal A(config)# ip multicast routing A(config)# interface GigabitEthernet 0/1 A(config-if)# ip pim dense mode A(config-if)# exit A(config)# interface GigabitEthernet 0/2 A(config-if)# ip pim dense mode A(config-if)# exit</pre>
<p>B</p>	<pre>B# configure terminal B(config)# ip multicast routing B(config)# interface GigabitEthernet 0/1 B(config-if)# ip pim dense mode B(config-if)# exit B(config)# interface GigabitEthernet 0/2 B(config-if)# ip pim dense mode B(config-if)# exit</pre>
<p>Verification</p>	<p>Enable the multicast source (192.168.1.100) to send packets to G (233.3.3.3). Enable receiver A to join G.</p> <ul style="list-style-type: none"> ➤ Check multicast packets received by receiver A. Receiver A should be able to receive multicast packets from G.

➤ Check multicast forwarding tables on A and B.	
A	<pre>A# show ip mroute IP Multicast Routing Table Flags: I Immediate Stat, T Timed Stat, F Forwarder installed, R RPT, S SPT, s SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.3), uptime 00:01:55, stat expires 00:02:19 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (1)</pre>
B	<pre>B# show ip mroute IP Multicast Routing Table Flags: I Immediate Stat, T Timed Stat, F Forwarder installed, R RPT, S SPT, s SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.3), uptime 00:00:35, stat expires 00:02:55 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1 (1)</pre>

Common Errors

- An IPv4 unicast route is incorrectly configured.
- IPv4 multicast routing is not enabled on a router.
- IP multicasting is not enabled on an interface.

1.4.2 Configuring a TTL Threshold

Configuration Effect

- Configure a TTL threshold for an interface and check the TTL values of multicast packets. Multicast packets whose TTL values are larger than the TTL threshold of the interface are forwarded and those whose TTL values are smaller are discarded.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- Set a TTL threshold on PIM router interfaces unless otherwise specified.

Verification

Enable multicast sources to send multicast packets and user hosts to join the groups.

- Set a TTL threshold to a value that is larger than the TTL value of the multicast packet on the PIM router interface directly connected to the user host and check whether the user can receive the multicast packet.

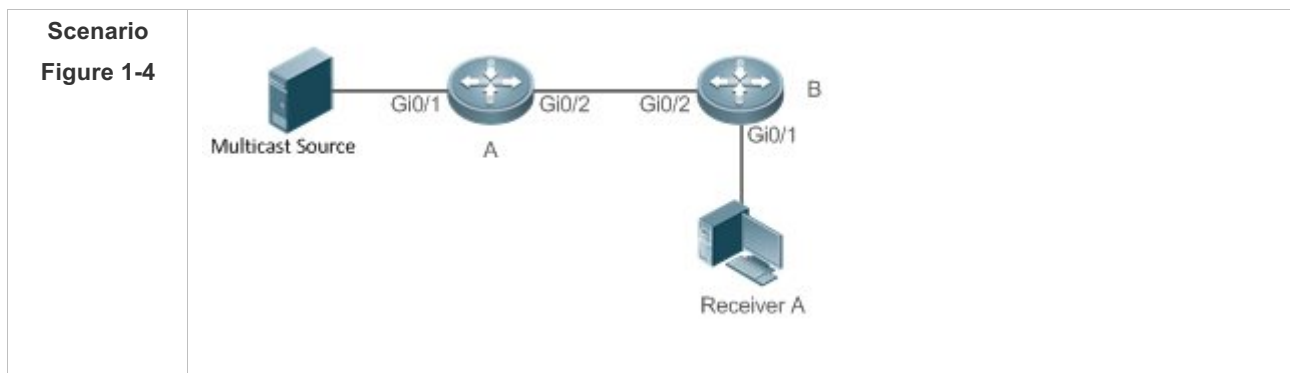
Related Commands

- ❖ Configuring a TTL Threshold

Command	<code>ip multicast ttl-threshold <i>ttl-value</i></code>
Parameter Description	<i>ttl-value</i> : Specifies a TTL threshold for an interface. The value ranges from 0 to 255. The default value is 0.
Command Mode	Interface configuration mode
Usage Guide	A multicast-enabled device can retain a TTL threshold for each interface. Multicast packets whose TTL values are larger than the TTL threshold of the interface are forwarded and those whose TTL values are smaller are discarded. A TTL threshold takes effect only for multicast frames and must be configured on layer-3 interfaces.

Configuration Example

- ❖ Creating the IP Multicast Service on the IPv4 Network and Configuring a TTL Threshold



Configuration Steps	<ul style="list-style-type: none"> ➤ Configure the basic functions of IP multicasting. (Omitted) ➤ Configure the TTL threshold as 100 on the Gi 0/2 interface of device A.
A	<pre>A# configure terminal A(config)#int gigabitEthernet 0/2 A(config-if GigabitEthernet 0/2)#ip multicast ttl threshold 100 A(config-if GigabitEthernet 0/2)# exit</pre>
Verification	<p>Enable the multicast source (192.168.1.100) to send packets to G (233.3.3.3). Enable receiver A to join G.</p> <ul style="list-style-type: none"> ➤ Configure the TTL threshold as 100 on the Gi 0/2 interface of device A, which is larger than the TTL value of the multicast packet. ➤ Check the difference between the route forwarding entries before and after the TTL threshold is configured.
Before Configuring the TTL Threshold	<pre>A# show ip mroute IP Multicast Routing Table Flags: I Immediate Stat, T Timed Stat, F Forwarder installed, R RPT, S SPT, s SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.3), uptime 00:00:08, stat expires 00:03:29 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (1)</pre>
After Configuring the TTL Threshold	<pre>A# show ip mroute IP Multicast Routing Table Flags: I Immediate Stat, T Timed Stat, F Forwarder installed, R RPT, S SPT, s SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL)</pre>

```
(192.168.1.100, 233.3.3.3), uptime 00:00:01, stat expires 00:03:29  
Owner PIMDM, Flags: TFS  
Incoming interface: GigabitEthernet 0/1  
Outgoing interface list:  
GigabitEthernet 0/2 (100)
```

1.4.3 Configuring the Number of Entries That Can Be Added to the Multicast Routing Table

Configuration Effect

- Each multicast data packet received on the device maintains a corresponding IP multicast route forwarding entry. However, excess multicast routing entries may exhaust device memory and deteriorate device performance. You can limit the number of entries in the IP multicast routing table based on the actual network and service performance requirements.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- Limit the number of entries in the IP multicast routing table based on the actual network and service performance requirements.

Verification

Send N groups of multicast packets from the multicast source on the network, configure user hosts to join the groups, configure the number of entries that can be added to the IP multicast routing table as N-1, and check whether the multicast packet received by the user host is that of the N-1 group.

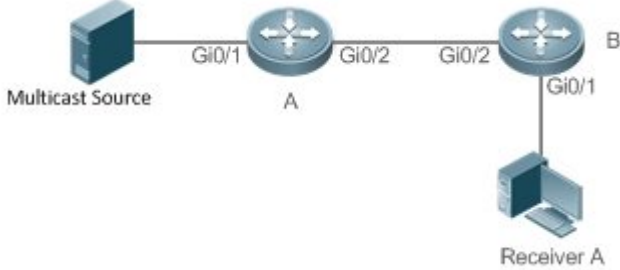
Related Commands

- ❖ Configuring the Number of Entries That Can Be Added to the Multicast Routing Table

Command	<code>ip multicast route-limit limit [threshold]</code>
Parameter Description	<i>limit</i> : Specifies the number of entries in the multicast routing table. The value ranges from 1 to 65536. The default value is 1024. <i>threshold</i> : Specifies the number of entries in the multicast routing table that triggers the warning message. The default value is 65536.
Command Mode	Global configuration mode
Usage Guide	Due to limitations on hardware resources, routing entries that exceed the range permitted by hardware can be forwarded only by software, deteriorating the performance.

Configuration Example

- ❖ Creating the IP Multicast Service on the IPv4 Network and Configuring the Number of Entries That Can Be Added to the Multicast Routing Table

<p>Scenario Figure 1-5</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure basic the functions of IP multicasting. (Omitted) ➤ Configure the number of entries that can be added to the multicast routing table on device B as 2.
<p>B</p>	<pre>B# configure terminal B(config)# ip multicast route limit 2</pre>
<p>Verification</p>	<p>Enable the multicast source (192.168.1.100) to send packets to G1 (233.3.3.1), G2 (233.3.3.2), and G3 (233.3.3.3). Enable receiver A to join G1, G2, and G3.</p> <ul style="list-style-type: none"> ➤ Check multicast packets received by receiver A. Receiver A should be able to receive multicast packets from two groups among G1, G2, and G3. ➤ Check multicast routing entries on A and B. ➤ When the number of entries in the IP multicasting routing table reaches the upper threshold, a prompt message is displayed.
<p>A</p>	<pre>A# show ip mroute IP Multicast Routing Table Flags: I Immediate Stat, T Timed Stat, F Forwarder installed, R RPT, S SPT, s SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.1), uptime 00:00:06, stat expires 00:03:24 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list:</pre>

	<pre>GigabitEthernet 0/2 (1) (192.168.1.100, 233.3.3.2), uptime 00:00:05, stat expires 00:03:25 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (1) (192.168.1.100, 233.3.3.3), uptime 00:00:00, stat expires 00:03:30 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (1)</pre>
B	<pre>B# show ip mroute IP Multicast Routing Table Flags: I Immediate Stat, T Timed Stat, F Forwarder installed, R RPT, S SPT, s SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (TTL) (192.168.1.100, 233.3.3.1), uptime 00:01:13, stat expires 00:03:23 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1 (1) (192.168.1.100, 233.3.3.3), uptime 00:06:08, stat expires 00:03:23 Owner PIMDM, Flags: TFS Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1 (1)</pre>

When the number of entries in the IP multicasting routing table reaches the upper threshold, a prompt message is displayed.

```
B#*Dec 26 10:43:07: %MROUTE 4 ROUTELIMIT: IPv4 Multicast route  
limit 2 exceeded VRF default.
```

Common Errors

- An IPv4 unicast route is incorrectly configured.

1.4.4 Configuring an IP Multicasting Border

Configuration Effect

- Configure an IP multicasting border to specify the transmission range of multicast packets.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- Configure an IP multicasting border on PIM router interfaces unless otherwise specified.

Verification

Enable multicast sources to send multicast packets and user hosts to join the groups. Configure an IP multicasting border on the PIM router interface connected to the user host and check whether the user can receive the multicast packet.


Related Commands

- ❖ Enabling IPv4 Multicast Routing

Command	<code>ip multicast boundary access-list [in out]</code>
Parameter	<i>access-list</i> : Indicates the group address range defined by ACL.
Description	<i>in</i> : Indicates that the IP multicasting border takes effect in the incoming direction of the multicast stream. <i>out</i> : Indicates that the IP multicasting border takes effect in the outgoing direction of the multicast stream.
Command Mode	Interface configuration mode
Usage Guide	After this command is executed, IGMP and PIM-SM packets in the group range are filtered on this interface and multicast data streams are not going in and out through this interface. The ACL associated with this command can be a standard ACL or an extended ACL. For extended ACLs, only the destination address is matched and the source address is matched.

Configuration Example

- ❖ Creating the IP Multicast Service on the IPv4 Network and Configuring an IP Multicasting Border

<p>Scenario Figure 1-6</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure the basic functions of IP multicasting. (Omitted) ➤ Configure an ACL on device A. ➤ Configure an IP multicasting border on the Gi 0/1 interface of device A.
<p>A</p>	<pre>A# configure terminal A(config)#ip access list standard ip_multicast A(config std nacl)#deny any A(config std nacl)#exit A(config)# interface GigabitEthernet 0/1 A(config if GigabitEthernet 0/1)#ip multicast boundary ip_multicast A A(config if GigabitEthernet 0/1)# exit</pre>
<p>Verification</p>	<p>Enable the multicast source (192.168.1.100) to send packets to G (233.3.3.3). Enable receiver A to join G.</p> <ul style="list-style-type: none"> ➤ Run debug ip pim sparse-mode events.
<p>A</p>	<pre>A# debug ip pim sparse mode events Jan 1 20:58:34: %7: VRF(0): No cache message: src 192.168.1.100 for 233.3.3.3 vif 2 *Jan 1 20:58:34: %7: VRF(0): Ignore No cache message: src 192.168.1.100 for 233.3.3.3 vif 2 in PIM_BOUNDARY_FLT_BOTH range</pre>

Common Errors

- An IPv4 unicast route is incorrectly configured.

1.4.5 Configuring an IP Multicasting Static Route

Configuration Effect

- Configure an IP multicasting static route to specify an RPF interface or RPF neighbor for multicast packets from specified multicast sources.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- An IP multicasting static route can be configured on each device unless otherwise specified.

Verification

Run **show ip rpf** { *source-address* [*group-address*] [**rd route-distinguisher**] } [**metric**] to check the RPF information of a specified source.

Related Commands

❖ Configuring Basic Functions of IP Multicasting


Command	ip mroute <i>source-address mask</i> { [bgp isis ospf rip static] { <i>v4rpf-address</i> <i>interface-type interface-number</i> } } [<i>distance</i>]
Parameter Description	<p><i>source-address</i>: Specifies the multicast source address.</p> <p><i>mask</i>: Specifies the mask of the multicast source address.</p> <p><i>protocol</i>: Indicates the unicast routing protocol currently used.</p> <p><i>rpf-address</i>: Specifies the address of the RPF neighbor (next hop of the multicast source).</p> <p><i>interface-type interface-number</i>: Indicates the RPF interface (outgoing interface of the multicast source).</p> <p><i>distance</i>: Specifies the route management distance. The value ranges from 0 to 255. The default value is 0.</p>
Command Mode	Global configuration mode
Usage Guide	<p>Multicast static routes are applicable only to RPF check.</p> <p>If the IP address of the outgoing interface, but not the next hop, of the static multicast route needs to be specified, the outgoing interface must be a point-to-point type.</p>

❖ Displaying the RFP Information of a Specified Source Address

Command	show ip rpf { <i>source-address</i> [<i>group-address</i>] [rd route-distinguisher] } [metric]
Parameter Description	<p><i>source-address</i>: Specifies the source IP address.</p> <p><i>group-address</i>: Specifies the group IP address.</p> <p>rd route-distinguisher: Indicates that the RD proxy is used for search.</p> <p>metric: Displays the metric of the MDT-SAFI route.</p>
Command Mode	Privilege, global and interface configuration modes
Usage Guide	<p>The three parameters are optional, and the source address and group address must be specified simultaneously.</p> <p>When no source address or group address is specified, all MFC entries are displayed.</p> <p>When only the source address and group address are specified, MFC entries of the source address and group address are displayed.</p>

Configuration Example

❖ Creating the IP Multicast Service on the IPv4 Network and Supporting PIM-DM

<p>Scenario Figure 1-7</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure the basic functions of IP multicasting. (Omitted) ➤ Configure a static route to the receiver on device B.
<p>A</p>	<pre>B# configure terminal B(config)# ip mroute 10.10.10.10 255.255.255.255 ospf 192.168.1.1 1</pre>
<p>Verification</p>	<p>Run show ip rpf to view the RPF information to the receiver before and after the configuration.</p>
<p>Before Configuration</p>	<pre>B# show ip rpf 10.10.10.10 RPF information for 10.10.10.10 RPF interface: GigabitEthernet 0/2 RPF neighbor: 192.168.2.1 RPF route: 10.10.10.10/32 RPF type: unicast (ospf) RPF recursion count: 0 Doing distance preferred lookups across tables Distance: 110 Metric: 1</pre>
<p>After Configuration</p>	<pre>B# show ip rpf 10.10.10.10 RPF information for 10.10.10.10 RPF interface: GigabitEthernet 0/0 RPF neighbor: 192.168.1.1 RPF route: 10.10.10.10/32 RPF type: static RPF recursion count: 0 Doing distance preferred lookups across tables Distance: 1</pre>

Metric: 0

Common Errors

- An IPv4 unicast route is incorrectly configured.
- IPv4 multicast routing is not enabled on a router.

1.4.6 Configuring Layer-2 Direction Control for Multicast Streams

Configuration Effect

Configure layer-2 direction control for multicast streams to control the forwarding of multicast streams on an interface.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- Layer-2 direction control for multicast streams can be configured on layer-2 devices unless otherwise specified.

Verification

Send multicast packets on the network containing layer-2 device A, connect multiple user hosts to VLAN 1 of layer-2 device A to receive the group, configure layer-2 direction control for multicast streams on device A, and check whether multicast packets are sent to the configured layer-2 interface.

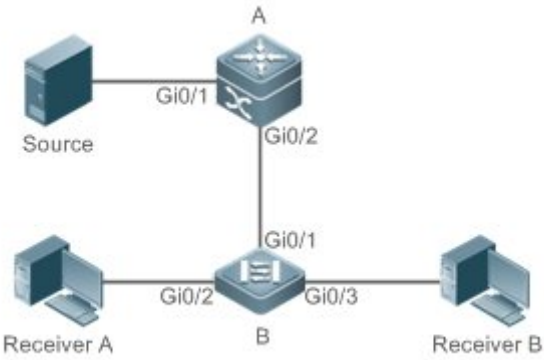
Related Commands

❖ Configuring Layer-2 Direction Control for Multicast Streams

Command	<code>ip multicast static source-address group-address interface-type interface-number</code>
Parameter Description	<i>source -address</i> : Specifies the multicast source address. <i>group-address</i> : Specifies the multicast group address. <i>interface-type interface-number</i> : Specifies a layer-2 interface that is allowed to forward the multicast flow.
Command Mode	Global configuration mode
Usage Guide	Allow a specified multicast flow to be configured with multiple commands, that is, to be configured with multiple interfaces. Once direction control is configured for a multicast stream, the stream can be forwarded only by these configured interfaces. Other interfaces are not permitted to forward the stream. This command controls only the forwarding of multicast streams on the interface, but does not directly affect the processing of multicast protocols on the protocol packets. However, since certain features of the multicast protocol are driven by multicast data streams, behaviors of the multicast routing protocols may also be affected.

Configuration Example

- ❖ Creating the IP Multicast Service on the IPv4 Network and Configuring Layer-2 Direction Control for Multicast Streams

<p>Scenario Figure 1-8</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure the basic functions of IP multicasting. (Omitted) ➤ Configure layer-2 direction control for multicast streams on device B so that the streams are sent only to the Gi 0/2 interface.
<p>B</p>	<pre>A# configure terminal A(config)# ip multicast static 192.168.1.100 233.3.3.3 gigabitEthernet0/2</pre>
<p>Verification</p>	<p>Enable the multicast source (192.168.1.100) to send packets to G (233.3.3.1). Enable receivers A and B to join G.</p> <ul style="list-style-type: none"> ➤ Check multicast packets received by receiver A. Receiver B should not be able to receive multicast packets from G.

Common Errors

- An IPv4 unicast route is incorrectly configured.

1.4.7 Configuring RPF Route Selection Based on the Longest Match Rule

Configuration Effect

- Select an optimal route respectively from the multicast static routing table, MBGP routing table, and unicast routing table and select the one with the longest match mask as the RPF route from the three optimal routes.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- Configure RPF route selection based on the longest match rule on each device unless otherwise specified.

Verification

Configure a multicast static route and a unicast static route to have the same priority and configure the unicast static route to have a longer mask length.

- Run **show ip rpf** { *source-address* [*group-address*] [*rd route-distinguisher*] } [*metric*] to check the RPF information of a specified source.

Related Commands

- ❖ Configuring RPF Route Selection Based on the Longest Match Rule

Command	ip multicast rpf longest-match
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	<p>The steps for selecting RFP routes are as follows:</p> <ol style="list-style-type: none"> 1. Select an optimal route respectively from the multicast static routing table, MBGP routing table, and unicast routing table for RPF check. 2. Select one from the three routes as the RPF route. <p>If the longest match rule is used, the route with the longest match mask is selected. If the three routes have the same mask, the one with the highest priority is selected. If they have the same priority, the RPF routes are selected in the sequence of multicast static route, MBGP route, and unicast route.</p> <p>If the longest match rule is not used, the route with the longest match mask is selected. If they have the same priority, the RPF routes are selected in the sequence of multicast static route, MBGP route, and unicast route.</p>

Configuration Example

- ❖ Creating the IP Multicast Service on the IPv4 Network and Configuring RPF Route Selection Based on the Longest Match Rule

Scenario Figure 1-9	
Configuration Steps	<ul style="list-style-type: none"> ➤ Configure the basic functions of IP multicasting. (Omitted) ➤ On device B, configure an IP multicast static route whose mask length is smaller than that of the unicast static route. ➤ Configure RPF route selection based on the longest match rule on device B.
B	<pre>B# configure terminal B(config)# ip multicast routing</pre>

	<pre>B(config)# ip mroute 10.10.10.10 255.255.0.0 ospf 192.168.1.1 B(config)# ip multicast rpf longest match</pre>
Verification	Run show ip rpf to check the RFP information of the multicast source before and after configuring RPF route selection based on the longest match rule.
Before configuration	<pre>B#show ip rpf 10.10.10.10 RPF information for 10.10.10.10 RPF interface: GigabitEthernet 0/0 RPF neighbor: 192.168.1.1 RPF route: 10.10.0.0/16 RPF type: static RPF recursion count: 0 Doing distance preferred lookups across tables Distance: 0 Metric: 0</pre>
After configuration	<pre>B# show ip rpf 10.10.10.10 RPF information for 10.10.10.10 RPF interface: GigabitEthernet 0/2 RPF neighbor: 192.168.2.1 RPF route: 10.10.10.10/32 RPF type: unicast (ospf) RPF recursion count: 0 Doing prefix length preferred lookups across tables Distance: 110 Metric: 1</pre>

Common Errors

- An IPv4 unicast route is incorrectly configured.
- IPv4 multicast routing is not enabled on a router.

1.4.8 Configuring Multicast Non-Stop Forwarding Parameters

Configuration Effect

- The non-stop forwarding function ensures continuous forwarding of multicast data streams during re-convergence of multicast protocols.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- ❖ Configuring the Maximum Period for Multicast Protocol Convergence
 - The maximum period for multicast protocol convergence can be specified on each device unless otherwise specified.
- ❖ Configuring the Multicast Packet Leakage Period
 - The multicast leakage period can be configured on each device unless otherwise specified.

Verification

Run **show msf nsf** to check the configured multicast non-stop forwarding parameters.

Related Commands

- ❖ Configuring the Maximum Period for Multicast Protocol Convergence

Command	msf nsf convergence-time <i>time</i>
Parameter Description	convergence-time <i>time</i> : Specifies the maximum period for multicast protocol convergence. The value ranges from 0 to 3600s. The default value is 20s.
Command Mode	Global configuration mode
Usage Guide	-

- ❖ Configuring the Multicast Packet Leakage Period

Command	msf nsf leak <i>interval</i>
Parameter Description	leak <i>interval</i> : Specifies the multicast packet leakage period. The value ranges from 0 to 3600s. The default value is 30s.
Command Mode	Global configuration mode
Usage Guide	-

- ❖ Displaying Multicast Non-Stop Forwarding Configurations

Command	show msf nsf
Parameter Description	-
Command Mode	Privilege, global and interface configuration modes
Usage Guide	-

Configuration Example

❖ Creating the IP Multicast Service on the IPv4 Network and Supporting PIM-DM

Scenario	Basic environment of the IP multicasting service (Omitted)
Configuration Steps	<ul style="list-style-type: none"> ➤ Configure the basic functions of IP multicasting. (Omitted) ➤ Configure the maximum period for multicast protocol convergence. ➤ Configure the multicast packet leakage period.
A	<pre>A# configure terminal A(config)# msf nsf convergence time 200 A(config)# msf nsf leak 300</pre>
Verification	Run show msf nsf to display multicast non-stop forwarding configurations.
A	<pre>A# show msf nsf Multicast HA Parameters + protocol convergence timeout 200 secs flow leak interval 300 secs</pre>

1.4.9 Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries

Configuration Effect

- Delete the earliest hardware entries and adds new entries if the hardware forwarding table overflows when you create multicast forwarding entries.

Notes

- The basic functions of IP multicasting must be configured.

Configuration Steps

- The overwriting mechanism upon overflow of multicast hardware forwarding entries can be configured on each device unless otherwise specified.

Verification

Run **show running-config** to check whether the overwriting mechanism upon overflow of multicast hardware forwarding entries is configured.

Related Commands

- ❖ Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries

Command	msf ipmc-overflow override
----------------	-----------------------------------

Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	-

Configuration Example

- ❖ Creating the IP Multicast Service on the IPv4 Network and Configuring an Overwriting Mechanism Upon Overflow of Multicast Hardware Forwarding Entries

Scenario	Basic environment of the IP multicasting service (Omitted)
Configuration Steps	<ul style="list-style-type: none"> ➤ Configure the basic functions of IP multicasting. (Omitted) ➤ Configure the overwriting mechanism upon overflow of multicast hardware forwarding entries.
A	<pre>A# configure terminal A(config)#msf ipmc overflow override</pre>
Verification	Run show running-config to check whether the overwriting mechanism upon overflow of multicast hardware forwarding entries is configured.
A	<pre>A# show running config ... msf ipmc overflow override ...</pre>

1.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and interrupt services.

Description	Command
Clears the IPv4 multicast forwarding table.	clear ip mroute { * <i>v4group-address</i> [<i>v4source-address</i>] }
Resets statistics in the IPv4 multicast forwarding table.	clear ip mroute statistics { * <i>v4group-address</i> [<i>v4source-address</i>] }

Displaying

Description	Command
Displays help guidance information of each multicast module.	multicast help

Description	Command
Displays status of the IPv4 multicast modules.	view multicast
Displays the IPv4 multicast forwarding table.	show ip mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]] [<i>dense</i> <i>sparse</i>] [<i>summary</i> <i>count</i>]
Displays IPv4 static multicast route information.	show ip mroute static
Displays the RFP Information of a specified IPv4 source address.	show ip rpf { <i>source-address</i> [<i>group-address</i>] [<i>rd route-distinguisher</i>] } [<i>metric</i>]
Displays information about IPv4 multicast interfaces.	show ip mvif [<i>interface-type interface-number</i>]
Displays the IPv4 layer-3 multicast forwarding table.	show ip mrf mfc
Displays the IPv4 multi-layer multicast forwarding table.	show msf msc
Displays IPv4 multicast non-stop forwarding configurations.	show msf nsf

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs running of the multicast core.	debug nsm mcast all
Debugs communication between the IPv4 multicast core and the protocol module.	debug nsm mcast fib-msg
Debugs the interface running of the IPv4 multicast core.	debug nsm mcast vif
Debugs the interface and entry statistics processing of the IPv4 multicast core.	debug nsm mcast stats
Debugs the processing of IPv4 layer-3 multicast packet forwarding.	debug ip mrf forwarding
Debugs the operation on layer-3 multicast forwarding entries on an IPv4 network.	debug ip mrf mfc
Debugs the processing of layer-3 multicast forwarding events on an IPv4 network.	debug ip mrf event

Description	Command
Debugs the processing of IPv4 multi-layer multicast packet forwarding.	debug msf forwarding
Debugs the operation on multi-layer multicast forwarding entries on an IPv4 network.	debug msf mfc
Debugs the bottom-layer hardware processing of IPv4 multi-layer multicast packet forwarding.	debug msf ssp
Debugs the invocation of API interfaces provided by IPv4 multi-layer multicast forwarding.	debug msf api
Debugs the processing of multi-layer multicast forwarding events on an IPv4 network.	debug msf event

2. CONFIGURING IPV6 MULTICAST

2.1 Overview

IPv6 multicast is enrichment and enhancement of IPv4 multicast. In comparison with IPv4 multicast, the IPv6 multicast address mechanism is greatly enriched.

In traditional IP transmission, a host is allowed to send packets only to a single host (unicast communication) or all hosts (broadcast communication). The multicast technology provides a third choice: A host is allowed to send packets to certain hosts.

The IP multicast technology is applicable to one-to-many multimedia applications.

Protocols and Standards

IPv6 multicast covers the following protocols:

- Multicast Listener Discovery (MLD): Runs between a multicast device and a host, and tracks and learns relationships of group members.
- Protocol Independent Multicast – Sparse Mode for IPv6 (PIM-SMv6): Runs between devices and implements multicast packet forwarding by establishing a multicast routing table.

2.2 Applications

Application	Description
Typical Application of PIM-SMv6	The PIM-SMv6 multicast service is provided in the same network.

2.2.1 Typical Application of PIM-SMv6

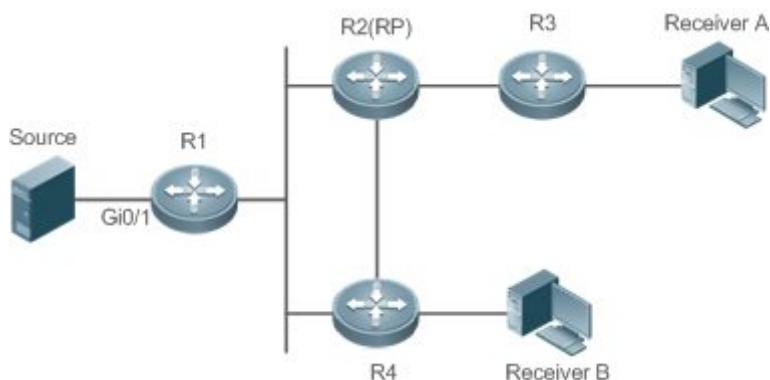
Scenario

The PIM-SMv6 multicast service is provided in the same network.

As shown in the following figure:

- R1 and the multicast source are in the same network, R2 is configured as a rendezvous point (RP), R3 is in the same network as Receiver A, and R4 is in the same network as Receiver B. Assume that devices and hosts are correctly connected, IPv6 is enabled on each interface, and IPv6 unicast is enabled on each device.

Figure 2-1



Remarks	<p>R1, R2, R3, and R4 are Layer-3 devices and R2 functions as an RP.</p> <p>The multicast source is directly connected to R1, Receiver A is directly connected to R3, and Receiver B is directly connected to R4.</p>
----------------	---

Deployment

- Run the Open Shortest Path First for IPv6 (OSPFv6) protocol in the same network to implement unicast routing.
- Run the PIM-SMv6 protocol in the same network to implement multicast routing.

2.3 Features

Basic Concepts

❖ PIM Router and PIM Interface

Routers where the PIM protocol is enabled are called PIM routers. Interfaces where the PIM protocol is enabled are called PIM interfaces.

Multicast packets are forwarded by PIM routers. The PIM interfaces for receiving multicast packets are called upstream interfaces, and the PIM interfaces for transmitting multicast packets are called downstream interfaces.

Network segments where upstream interfaces are located are called upstream network segments. Network segments where downstream interfaces are located are called downstream network segments.

❖ PIM Network and PIM Domain

PIM routers are connected through PIM interfaces and form a PIM network.

On some PIM interfaces, borders are set to divide a large PIM network into multiple PIM domains. The borders may reject specific multicast packets or limit transmission of PIM messages.

❖ Multicast Distribution Tree, DR, RP

Multicast packets are transmitted from one point to multiple points. The forwarding path presents a tree structure. This forwarding path is called a multicast distribution tree (MDT). MDTs are classified into two types:

- Rendezvous point tree (RPT): Uses the rendezvous point (RP) as the root and designated routers (DRs) connected to group members as leaves.
- Shortest path tree (SPT): Use the DR connected to a multicast source as the root and the RPs or DRs connected to group members as leaves.

DRs and RPs are function roles of PIM routers.

- RPs collect information about multicast sources and group members in the network.
- The DR connected to a multicast source reports multicast source information to the RP and the DRs connected to group members report the group member information to the RP.

❖ (*,G), (S,G)

- (*,G): Indicates the packets transmitted from any source to Group G, routing entries corresponding to the packets, and forwarding path (RPT) corresponding to the packets.
- (S,G): Indicates the packets transmitted from Source S to Group G, routing entries corresponding to the packets, and forwarding path (SPT) corresponding to the packets.

❖ ASM, SSM

PIM-SM supports two multicast service models: any-source multicast (ASM) and source-specific multicast (SSM), which are applicable to different multicast address segments.

- ASM: In the ASM model, a user host cannot select a multicast source. The user host joins a multicast group and receives all packets sent from all sources to the multicast group.
 - SSM: In the SSM model, a user host can select a multicast source. The user host specifies the source address when joining a multicast group, and then receives packets only from the specified source to the multicast group.
-
- SSM model requirement: Other network services must be used to enable a user host to know the position of a multicast source in advance so that the user host selects the multicast source.

Overview

Feature	Description
Configuring IPv6 Multicast Basic Functions	Creates a PIM network to provide the IPv6 multicast service for data sources and user terminals in the network.
Configuring the Number of Entries That Can Be Added to the IPv6 Multicast Routing Table	Restricts the number of entries that can be added to the multicast routing table.

Feature	Description
Configuring the IPv6 Multicast Border	Sets an interface as the multicast border of a specific group range.
Configuring IPv6 Multicast Static Routing	Configures multicast static routing to adopt multicast forwarding paths different from unicast forwarding paths.
Configuring Layer-2 Flow Direction Control for Multicast Streams	Multiple commands can be configured for a multicast stream, that is, multiple ports can be allowed to forward the multicast stream. If flow direction control is configured for a multicast stream, the multicast stream can be forwarded only by the configured ports. Other ports are not allowed to forward the multicast stream.
Configuring RPF Route Selection According to the Longest Matching Principle	One optimal route is selected from each of the multicast static routing table, MBGP routing table, and unicast routing table according to RPF rules. Among the three optimal routes, the route with the longest subnet mask matching is selected as the RPF route.

2.3.1 Configuring IPv6 Multicast Basic Functions

Create a PIM network to provide the IPv6 multicast service for data sources and user terminals in the network.

Working Principle

A device maintains the routing table used for multicast packet forwarding over an IPv6 multicast routing protocol (such as PIM-SMv6), and learns information about the status of group members in the directly-connected network segments over the MLDv1/v2 protocol. A host joins a specific IPv6 multicast group by transmitting the MLD REPORT message.

Related Configuration

❖ Enabling the IPv6 Multicast Routing Function

The IPv6 multicast routing function is disabled by default.

Run the **ipv6 multicast-routing** command to enable the IPv6 multicast routing function.

❖ Configuring an IP Multicast Protocol on an Interface

The IPv6 multicast protocol is disabled on an interface by default.

Run the **ipv6 pim dense-mode** command to enable the IPv6 multicast protocol on an interface.

2.3.2 Configuring the Number of Entries That Can Be Added to the IPv6 Multicast Routing Table

Every multicast data packet received by the device is used to maintain relevant IPv6 multicast routing entries. Excessive multicast routing entries, however, may deplete the device memory and degrade the device performance. Users can restrict the number of entries in the IPv6 multicast routing table based on the actual networking conditions and service performance requirements.

Working Principle

Restrict the number of entries in the IPv6 multicast routing table based on the actual networking conditions and service performance requirements, so as to sustain the device performance.

Related Configuration

- ❖ Configuring the Number of Entries That Can Be Added to the IPv6 Multicast Routing Table

By default, 1,024 entries can be added to the IP multicast routing table.

Run the **ipv6 multicast route-limit** *limit* [*threshold*] command to adjust the number of entries that can be added to the IPv6 multicast routing table. The value ranges from 1 to 65,536.

A larger value of *limit* means that more entries can be added to the IPv6 multicast routing table, and a smaller value of *limit* means that fewer entries can be added to the IPv6 multicast routing table.

2.3.3 Configuring the IPv6 Multicast Border

Configure the IPv6 multicast border to restrict the transmission scope of multicast packets.

Working Principle

Configure the multicast border to specify the transmission scope of multicast packets. When the multicast forwarding border is configured on an interface, multicast packets including multicast packets sent by the local device cannot be forwarded or received by this interface.

Related Configuration

- ❖ Configuring the IPv6 Multicast Border

No multicast border is configured by default.

Run the **ipv6 multicast boundary** *access-list-name* [**in** | **out**] command to configure the multicast border.

2.3.4 Configuring IPv6 Multicast Static Routing

Configure IPv6 multicast static routing to specify a reverse path forwarding (RPF) interface or RPF neighbor for multicast packets from a specific multicast source.

Working Principle

The RPF check is conducted during forwarding of multicast packets. IPv6 multicast static routing can be configured to specify an RPF interface or RPF neighbor for multicast packets from a specific multicast source.

Related Configuration

- ❖ Configuring IPv6 Multicast Static Routing

No multicast static routing is configured by default.

Run the **ipv6 mroute** *ipv6-prefix/prefix-length* [**bgp** | **isis** | **ospfv3** | **ripng** | **static**] { *ipv6-prefix* | *interface-type interface-number* } [*distance*] command to configure IPv6 multicast static routing.

2.3.5 Configuring Layer-2 Flow Direction Control for Multicast Streams

Configure Layer-2 flow direction control for multicast streams to control the forwarding behavior of multicast streams on ports.

Working Principle

Configure Layer-2 flow direction control for multicast streams to configure the ports that are allowed to forward multicast streams. Then, multicast streams are forwarded only by the configured ports, thereby controlling Layer-2 forwarding of multicast streams.

Related Configuration

❖ Configuring Layer-2 Flow Direction Control for Multicast Streams

Layer-2 flow direction control is disabled for multicast streams by default.

Run the **ipv6 multicast static** *source-address group-address interface-type interface-number* command to configure the Layer-2 flow direction control for multicast streams.

2.3.6 Configuring RPF Route Selection According to the Longest Matching Principle

Among the three optimal routes selected from the multicast static routing table, Multiprotocol Border Gateway Protocol (MBGP) routing table, and unicast routing table, select the optimal route with the longest subnet mask matching as the RPF route.

Working Principle

According to RPF rules, select a multicast static route, MBGP route, and unicast route used for the RPF check respectively from the multicast static routing table, MBGP routing table, and unicast routing table.

- If route selection according to the longest matching principle is configured, the route with the longest subnet mask matching is selected out of the three routes as the RPF route. If the three routes share the same subnet mask, the route with the highest priority is selected. If the three routes have the same priority, the RPF route is selected according to the sequence of multicast static route, MBGP route, and unicast route.
- If route selection according to the longest matching principle is not configured, the route with the highest priority is selected. If the three routes have the same priority, the RPF route is selected according to the sequence of multicast static route, MBGP route, and unicast route.

Related Configuration

❖ Configuring RPF Route Selection According to the Longest Matching Principle

A route with the highest priority is selected as the RPF route by default. If the routes have the same priority, the RPF route is selected according to the sequence of multicast static route, MBGP route, and unicast route.

Run the **ipv6 multicast rpf longest-match** command to configure RPF route selection according to the longest matching principle.

2.4 Configuration

Configuration	Description and Command	
Configuring IPv6 Multicast Basic Functions	(Mandatory) It is used to create a multicast service.	
	ipv6 multicast-routing	Enables the IPv6 multicast routing function.
Configuring the Number of Entries That Can Be Added to the IPv6 Multicast Routing Table	Optional.	
	ipv6 multicast route-limit <i>limit</i> [<i>threshold</i>]	Restricts the number of entries that can be added to the multicast routing table.
Configuring the IPv6 Multicast Border	ipv6 multicast boundary <i>access-list-name</i> [<i>in</i> <i>out</i>]	Sets an interface as the multicast border of a specific group range.
Configuring IPv6 Multicast Static Routing	ipv6 mroute <i>ipv6-prefix/prefix-length</i> [<i>protocol</i>] { <i>v6rpf-address</i> <i>interface-type interface-number</i> } [<i>distance</i>]	Configures IPv6 multicast static routing.
Configuring Layer-2 Flow Direction Control for Multicast Streams	ipv6 multicast static <i>source-address group-address interface-type interface-number</i>	Controls the flow direction of data streams on Layer-2 ports.
Configuring RPF Route Selection According to the Longest Matching Principle	ipv6 multicast rpf longest-match	Configures RPF route selection according to the longest matching principle.

2.4.1 Configuring IPv6 Multicast Basic Functions

Configuration Effect

- Create a PIM network to provide the IPv6 multicast service for data sources and user terminals in the network.

Notes

- The PIM network needs to use existing unicast routing in the network. Therefore, IPv6 unicast routing must be configured in the network.

Configuration Steps

- ❖ Enabling the IPv6 Multicast Routing Function
 - Mandatory.
 - Enable the IPv6 multicast routing function on each router unless otherwise specified.
- ❖ Enabling an IP Multicast Protocol on Interfaces
 - Mandatory.
 - Enable the IPv6 multicast protocol function on interfaces unless otherwise specified.

Verification

Make multicast sources in the network send multicast packets and make a user host join the groups.

- Check whether the user host can successfully receive packets from each group.

Related Commands

❖ Enabling the IPv6 Multicast Routing Function

Command	ipv6 multicast-routing
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The IPv6 multicast routing function must be enabled before various IPv6 multicast protocols are enabled. The IPv6 multicast routing function and the MLD snooping function are mutually exclusive.

❖ Configuring IPv6 Multicast Protocols

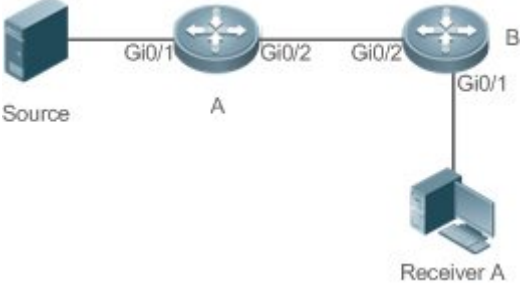
- For details about the MLD configuration method, see the *Configuring MLD*.
- For details about the PIM-SMv6 configuration method, see the *Configuring PIM-SMv6*.
- After the Layer-3 multicast function is enabled on a private VLAN and Super VLAN, if there is a multicast source in the sub-VLAN, an entry needs to be additionally copied, with the inlet of the sub-VLAN where multicast streams enter because the validity check needs to be conducted at the inlet during multicast packet forwarding. As a result, one more multicast hardware entry is occupied, and the multicast capacity needs to be decreased by one.

❖ Displaying Multicast Forwarding Table Information

Command	show ipv6 mroute [group-or-source-address [group-or-source-address]] [sparse] [summary count]
Parameter Description	<i>group-or-source-address</i> : Indicates the group address or source address. <i>group-or-source-address</i> : Indicates the group address or source address. sparse : Displays the core entry of the PIM-SMv6 multicast routing table. summary : Displays the summary of IPv6 multicast routing entries. count : Displays the count information about IPv6 multicast routing entries.
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	N/A

Configuration Example

❖ Creating the IPv6 Multicast Service on an IPv6 Network to Support PIMv6-SM

<p>Scenario Figure 2-2</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure an IPv6 unicast routing protocol (for example, OSPFv3) on routers. ➤ Enable the IPv6 multicast routing function on all routers. ➤ Enable the PIMv6-SM function on device interconnection interfaces, interface for connecting to the user host, and interface for connecting to the multicast source.
<p>A</p>	<pre>A# configure terminal A(config)# ipv6 multicast routing A(config)# interface gigabitEthernet 0/1 A(config if GigabitEthernet 0/1)#ipv6 pim sparse mode A(config if)# exit A(config)# interface gigabitEthernet 0/2 A(config if GigabitEthernet 0/2)#ipv6 pim sparse mode A(config if)# exit</pre>
<p>B</p>	<pre>B# configure terminal B(config)# ipv6 multicast routing B(config)# interface gigabitEthernet 0/1 B(config if GigabitEthernet 0/1)#ipv6 pim sparse mode B(config if)# exit B(config)# interface GigabitEthernet 0/2 B(config if GigabitEthernet 0/2)#ipv6 pim sparse mode B(config if)# exit</pre>
<p>Verification</p>	<p>Make Multicast Source (2001::1) send packets to G(ff16::16) and make Receiver A join G.</p> <ul style="list-style-type: none"> ➤ Check multicast packets received by Receiver A. Receiver A should be able to receive multicast packets from G. ➤ Check the multicast forwarding table on Receiver A and Device B.

A	<pre>A# show ipv6 mroute IPv6 Multicast Routing Table Flags: I Immediate Stat, T Timed Stat, F Forwarder installed, R RPT, S SPT, s SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (2001::1, ff16::16), uptime 00:03:12, stat expires 00:02:03 Owner PIMSMV6, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2</pre>
B	<pre>B# show ipv6 mroute IPv6 Multicast Routing Table Flags: I Immediate Stat, T Timed Stat, F Forwarder installed, R RPT, S SPT, s SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (2001::1, ff16::16), uptime 00:00:23, stat expires 00:03:07 Owner PIMSMV6, Flags: TFR Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1</pre>

Common Errors

- IPv6 unicast routing is incorrectly configured.
- IPv6 multicast routing is not enabled on a router.
- No IPv6 multicast protocol is enabled on an interface.

2.4.2 Configuring the Number of Entries That Can Be Added to the IPv6 Multicast Routing Table

Configuration Effect

- Every multicast data packet received by the device is used to maintain relevant IPv6 multicast routing entries. Excessive multicast routing entries, however, may deplete the device memory and degrade the device performance. Users can restrict the number of entries in the IPv6 multicast routing table based on the actual networking conditions and service performance requirements.

Notes

- The IPv6 multicast basic functions must be configured.

Configuration Steps

- Restrict the number of entries in the IPv6 multicast routing table based on the actual networking conditions and service performance requirements.

Verification

Make multicast sources in the network send multicast packets to N different multicast groups and make a user host join these groups. Set the number of entries that can be added to the IPv6 multicast routing table to N-1 on the device and check that multicast packets received by the user host are from N-1 groups.

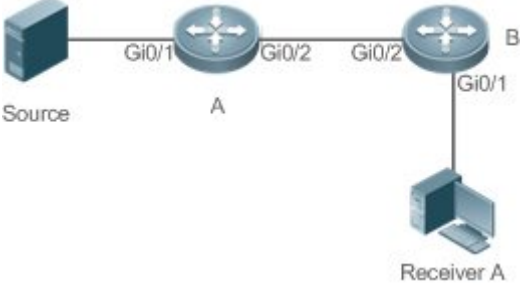
Related Commands

- ❖ Configuring the Number of Entries That Can Be Added to the IP Multicast Routing Table

Command	<code>ipv6 multicast route-limit limit [threshold]</code>
Parameter Description	<i>limit</i> : Indicates the number of multicast routing entries. The value ranges from 1 to 65,536 and the default value is 1,024. <i>threshold</i> : Indicates the multicast routing entry quantity for triggering an alarm. The default value is 65,536.
Command Mode	Global configuration mode
Usage Guide	Routing entries that are beyond the allowable range of hardware can be forwarded only by software due to hardware resource restrictions, making the performance deteriorate.

Configuration Example

- ❖ Creating the IPv6 Multicast Service on an IPv6 Network and Configuring the Number of Entries That Can Be Added to the IPv6 Multicast Routing Table

<p>Scenario Figure 2-3</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure IP multicast basic functions (omitted). ➤ Set the number of entries that can be added to the IP multicast routing table to 2 on Device B.
<p>B</p>	<pre>B# configure terminal B(config)# ipv6 multicast route limit 2</pre>
<p>Verification</p>	<p>Make Multicast Source (2001::1) send packets to G1(ff16::16), G2(ff16::17), and G3(ff16::18) and make Receiver A join G1, G2, and G3.</p> <ul style="list-style-type: none"> ➤ Check multicast packets received by Receiver A. Receiver A should be able to receive multicast packets from two groups of G1, G2, and G3. ➤ Check multicast routing entries on Receiver A and Device B. ➤ A prompt is displayed when the number of entries in the multicast routing table reaches the upper limit.
<p>A</p>	<pre>A# show ipv6 mroute IPv6 Multicast Routing Table Flags: I Immediate Stat, T Timed Stat, F Forwarder installed, R RPT, S SPT, s SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (2001::1, ff16::16), uptime 00:01:01, stat expires 00:02:29 Owner PIMSMV6, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2</pre>

	<pre>(2001::1, ff16::17), uptime 00:01:01, stat expires 00:02:29 Owner PIMSMV6, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2 (2001::1, ff16::18), uptime 00:00:57, stat expires 00:02:33 Owner PIMSMV6, Flags: TFS Incoming interface: GigabitEthernet 0/1 Outgoing interface list: GigabitEthernet 0/2</pre>
B	<pre>B# show ipv6 mroute IPv6 Multicast Routing Table Flags: I Immediate Stat, T Timed Stat, F Forwarder installed, R RPT, S SPT, s SSM Group Timers: Uptime/Stat Expiry Interface State: Interface (2001::1, ff16::16), uptime 00:00:29, stat expires 00:03:01 Owner PIMSMV6, Flags: TFR Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1 (2001::1, ff16::17), uptime 00:00:29, stat expires 00:03:01 Owner PIMSMV6, Flags: TFR Incoming interface: GigabitEthernet 0/2 Outgoing interface list: GigabitEthernet 0/1</pre>
A prompt is displayed when the	<pre>B#* Jan 3 21:40:07: %MROUTE 4 ROUTELIMIT: IPv6 Multicast route limit 2 exceeded..</pre>

number of entries in the multicast routing table reaches the upper limit.	
---	--

Common Errors

- IPv6 unicast routing is incorrectly configured.

2.4.3 Configuring the IPv6 Multicast Border

Configuration Effect

- Configure the IPv6 multicast border to restrict the transmission scope of multicast packets.

Notes

- The IPv6 multicast basic functions must be configured.

Configuration Steps

- Configure the IPv6 multicast border on each PIM router interface unless otherwise specified.

Verification

Make multicast sources send multicast packets to multicast groups and make a user host join these multicast groups. Configure the IPv6 multicast border on the PIM router interface connected to the user host and check whether the user host can receive multicast packets.

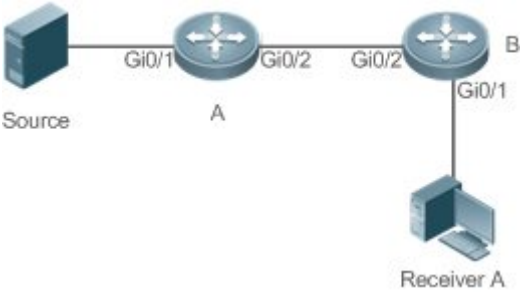
Related Commands

- ❖ Enabling the IPv6 Multicast Routing Function

Command	<code>ipv6 multicast boundary <i>access-list-name</i> [in out]</code>
Parameter Description	<i>access-list-name</i> : Uses the group address range defined by an access control list (ACL). in : Indicates that the multicast border takes effect in the incoming direction of multicast streams. out : Indicates that the multicast border takes effect in the outgoing direction of multicast streams.
Command Mode	Interface configuration mode
Usage Guide	The ACL referenced in this command can be a standard ACL or an extended ACL. If an extended ACL is used, only destination addresses need to be matched. This command can be used to filter MLD and PIM-SMv6 protocol packets relevant to the IPv6 multicast group range. Multicast data streams are not transmitted or received by multicast border interfaces.

Configuration Example

❖ Creating the IPv6 Multicast Service on an IPv6 Network and Configuring the IPv6 Multicast Border

<p>Scenario Figure 2-4</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure IP multicast basic functions (omitted). ➤ Configure an ACL on Device A. ➤ Configure the IP multicast border on Interface Gi0/1 of Device A.
<p>A</p>	<pre>A# configure terminal A(config)# ipv6 access list ip_multicast A(config ipv6 acl)#deny udp any any A(config ipv6 acl)#exit A(config)# interface GigabitEthernet 0/1 A(config if GigabitEthernet 0/1)#ip multicast boundary ip_multicast A A(config if GigabitEthernet 0/1)# exit</pre>
<p>Verification</p>	<p>Make Multicast Source (192.168.1.100) send packets to G (233.3.3.3) and make Receiver A join G.</p> <ul style="list-style-type: none"> ➤ Run the debug ipv6 pim sparse-mode events command to debug multicast events in SM mode.
<p>A</p>	<pre>A# debug ipv6 pim sparse mode events Dec 28 11:54:07: %7: No cache message: src 2001::1 for ff16::16 vif 1 *Dec 28 11:54:07: %7: Ignore No cache message: src 2001::1 for ff16::16 vif 1 in PIM6_BOUNDARY_FLT_BOTH range</pre>

Common Errors

- IPv6 unicast routing is incorrectly configured.

2.4.4 Configuring IPv6 Multicast Static Routing

Configuration Effect

- Configure IPv6 multicast static routing to specify an RPF interface or RPF neighbor for multicast packets from a specific multicast source.

Notes

- The IPv6 multicast basic functions must be configured.

Configuration Steps

- Configure IPv6 multicast static routing on each device unless otherwise specified.

Verification

Configure IPv6 multicast static routing and then run the **show ipv6 rpf v6source-address** command to check RPF information about a specific multicast source.

Related Commands

❖ Configuring IPv6 Multicast Static Routing

Command	<code>ipv6 mroute ipv6-prefix/prefix-length [protocol] { v6rpf-address interface-type interface-number } [distance]</code>
Parameter Description	<p><i>ipv6-prefix</i>: Indicates the IPv6 address of a multicast source.</p> <p><i>prefix-length</i>: Indicates the subnet mask of the IPv6 address of the multicast source.</p> <p><i>protocol</i>: Indicates the unicast routing protocol that is being used currently.</p> <p><i>v6rpf-address</i>: Indicates the IPv6 address of the RPF neighbor (next hop to the multicast source).</p> <p><i>interface-type interface-number</i>: Indicates the RPF interface (outbound interface to the multicast source).</p> <p><i>distance</i>: Indicates the route management distance. The value ranges from 0 to 255 and the default value is 0.</p>
Command Mode	Global configuration mode
Usage Guide	<p>IPv6 multicast static routing is used only for the RPF check.</p> <p>To specify the outbound interface rather than the next-hop IP address of IPv6 static multicast routing, the outbound interface must be of the point-to-point type.</p>

❖ Displaying RPF Information About a Specific Source Address

Command	<code>show ipv6 rpf v6source-address</code>
----------------	---

Parameter Description	<i>v6source-address</i> : Indicates the IPv6 source address.
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	N/A

Configuration Example

- ❖ Creating the IPv6 Multicast Service on an IPv6 Network and Configuring IPv6 Multicast Static Routing

Scenario Figure 2-5	
Configuration Steps	<ul style="list-style-type: none"> ➤ Configure IPv6 multicast basic functions (omitted). ➤ Configure a static route to the receiver on Device B.
A	<pre>B# configure terminal B(config)# ipv6 mroute 2005::/64 ospfv3 2002::2</pre>
Verification	Run the show ipv6 rpf command to display the RPF information received by the receiver before and after configuration.
Before Configuration	<pre>B# show ipv6 rpf 2005::1 RPF information for 2005::1 RPF interface: GigabitEthernet 0/1 RPF neighbor: fe80::2d0:f8ff:fe22:341b RPF route: 2005::1/128 RPF type: unicast (ospf) RPF recursion count: 0 Doing distance preferred lookups across tables Distance: 110 Metric: 1</pre>
After Configuration	<pre>B# show ipv6 rpf 2005::1 RPF information for 2005::1 RPF interface: GigabitEthernet 0/2 RPF neighbor: 2002::2</pre>


```
RPF route: 2005::/64
RPF type: unicast (ospf)
RPF recursion count: 0
Doing distance preferred lookups across tables
Distance: 110
Metric: 1
```

Common Errors

- IPv6 unicast routing is incorrectly configured.
- IPv6 multicast routing is not enabled on a router.

2.4.5 Configuring Layer-2 Flow Direction Control for Multicast Streams

Configuration Effect

Configure Layer-2 flow direction control for multicast streams to control the forwarding behavior of multicast streams on ports.

Notes

- The IPv6 multicast basic functions must be configured.

Configuration Steps

- Configure Layer-2 flow direction control for multicast streams on devices unless otherwise specified.

Verification

Make Device A send multicast packets to multicast groups in the network. Multiple user hosts connected to VLAN 1 of Device A receive multicast packets from these multicast groups. Configure Layer-2 flow direction control for multicast streams on Device A so that multicast packets are sent to configured ports.

Related Commands

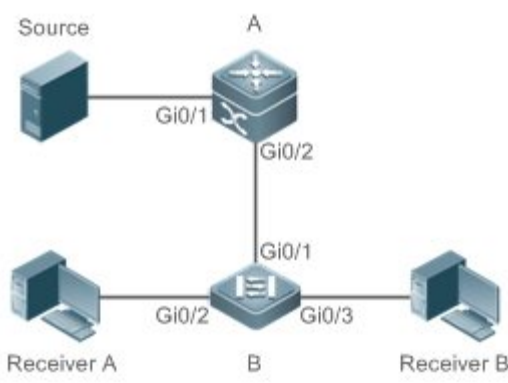
- ❖ Configuring Layer-2 Flow Direction Control for Multicast Streams

Command	<code>ipv6 multicast static source-address group-address interface-type interface-number</code>
Parameter Description	<i>source -address</i> : Indicates the multicast source address. <i>group-address</i> : Indicates the multicast group address. <i>interface-type interface-number</i> : Indicates a Layer-2 port that is allowed to forward multicast streams.
Command Mode	Global configuration mode
Usage Guide	Multiple commands can be configured for a multicast stream, that is, multiple ports can be allowed to forward the multicast stream. If flow direction control is configured for a multicast stream, the

	<p>multicast stream can be forwarded only by the configured ports. Other ports are not allowed to forward the multicast stream.</p> <p>This command controls only the forwarding behavior of multicast streams on ports. It does not directly affect processing of protocol packets by multicast protocols. Some features of multicast protocols (such as PIM-SMv6) are driven by multicast data streams, and therefore, the behavior of the multicast routing protocols may still be affected.</p>
--	---

Configuration Example

- ❖ Creating the IPv6 Multicast Service on an IPv6 Network and Configuring Layer-2 Flow Direction Control for Multicast Streams

<p>Scenario Figure 2-6</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure IP multicast basic functions (omitted). ➤ Configure Layer-2 flow direction control for multicast streams on Device B so that multicast streams are transmitted only to Interface Gi0/2.
<p>B</p>	<pre>A# configure terminal A(config)# ipv6 multicast static 2001::1 ff16::16 gigabitEthernet 0/2</pre>
<p>Verification</p>	<p>Make Multicast Source (2001::1) send packets to G (ff16::16) and make Receiver A and Receiver B join G.</p> <ul style="list-style-type: none"> ➤ Receiver A should be able to receive multicast packets from G but Receiver B cannot receive multicast packets from G.

Common Errors

- IPv6 unicast routing is incorrectly configured.

2.4.6 Configuring RPF Route Selection According to the Longest Matching Principle

Configuration Effect

Among the three optimal routes selected from the multicast static routing table, MBGP routing table, and unicast routing table, select the optimal route with the longest subnet mask matching as the RPF route.

Notes

- The IP multicast basic functions must be configured.

Configuration Steps

- Configure RPF route selection according to the longest matching principle on each device unless otherwise specified.

Verification

Configure a multicast static route and a unicast static route with the same priority and configure the unicast static route to have the longest subnet mask matching.

- Run the **show ipv6 rpf v6source-address** command to check RPF information about a specific source.

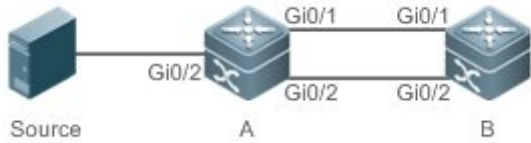
Related Commands

- ❖ Configuring RPF Route Selection According to the Longest Matching Principle

Command	ipv6 multicast rpf longest-match
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	<p>The steps of selecting an RPF route are as follows:</p> <p>Select one optimal route used for the RPF check from each of the IPv6 multicast static routing table, IPv6 MBGP routing table, and IPv6 unicast routing table.</p> <p>Select one route out of the three optimal routes as the RPF route.</p> <p>If the command for selecting the RPF route according to the longest matching principle is configured, the route with the longest subnet mask matching is selected out of the three optimal routes as the RPF route. If the three routes share the same subnet mask, the route with the highest priority is selected. If the routes have the same priority, the RPF route is selected according to the sequence of IPv6 multicast static route, IPv6 MBGP route, and IPv6 unicast route.</p> <p>If the command for selecting the RPF route according to the longest matching principle is not configured, the route with the highest priority is selected out of the three optimal routes as the RPF route. If the routes have the same priority, the RPF route is selected according to the sequence of IPv6 multicast static route, IPv6 MBGP route, and IPv6 unicast route.</p>

Configuration Example

- ❖ Creating the IPv6 Multicast Service on the IPv6 Network and Configuring the RPF Route Selection According to the Longest Matching Principle

<p>Scenario Figure 2-7</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure IP multicast basic functions (omitted). ➤ Configure an IPv6 multicast static route with the subnet mask length smaller than that of the unicast route on Device B. ➤ Configure the RPF route selection according to the longest matching principle on Device B.
<p>B</p>	<pre>B# configure terminal B(config)# ipv6 multicast routing B(config)# ipv6 mroute 205::/64 ospfv3 2002::2 B(config)# ipv6 multicast rpf longest match</pre>
<p>Verification</p>	<p>Run the show ipv6 rpf command to display the RPF information about the multicast source before and after RPF route selection according to the longest matching principle is configured.</p>
<p>Before Configuration</p>	<pre>B# show ipv6 rpf 205:::1 RPF information for 205:::1 RPF interface: GigabitEthernet 0/2 RPF neighbor: 2002::2 RPF route: 205::/64 RPF type: unicast (ospf) RPF recursion count: 0 Doing distance preferred lookups across tables Distance: 110 Metric: 1</pre>
<p>After Configuration</p>	<pre>B# show ipv6 rpf 205:::1 RPF information for 205:::1 RPF interface: GigabitEthernet 0/1 RPF neighbor: fe80::2d0:f8ff:fe22:341b RPF route: 205:::1/128 RPF type: unicast (ospf) RPF recursion count: 0</pre>

```
Doing distance preferred lookups across tables
Distance: 110
Metric: 1
```

Common Errors

- IPv6 unicast routing is incorrectly configured.
- IPv6 multicast routing is not enabled on a router.

2.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the IPv6 multicast forwarding table.	clear ipv6 mroute { * <i>v6group-address</i> [<i>v6source-address</i>] }
Clears the statistics in the IPv6 multicast forwarding table.	clear ipv6 mroute statistics { * <i>v6group-address</i> [<i>v6source-address</i>] }

Displaying

Description	Command
Displays the IPv6 multicast forwarding table information.	show ipv6 mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]] [sparse] [summary count]
Displays RPF information about a specific IPv6 source address.	show ipv6 rpf <i>v6source-address</i>
Displays information the IPv6 static multicast route.	show ipv6 mroute static
Displays information about the configured IPv6 multicast interface that takes effect.	show ipv6 mvif [<i>interface-type interface-number</i>]
Displays the IPv6 Layer-3 multicast forwarding table.	show ipv6 mrf mfc
Displays the IPv6 multi-layer multicast forwarding table.	show msf6 msc

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs all running processes of the IPv6 multicast.	debug nsm mcast6 all
Debugs the communication between the IPv6 multicast and the protocol module.	debug nsm mcast6 fib-msg
Debugs the interface running of the IPv6 multicast.	debug nsm mcast6 mif
Debugs the processing of interfaces and behavior statistics of the IPv6 multicast.	debug nsm mcast6 stats
Debugs the Layer-3 multicast forwarding of IPv6.	debug ipv6 mrf forwarding
Debugs the operation process of IPv6 Layer-3 multicast forwarding entries.	debug ipv6 mrf mfc
Debugs the processing of IPv6 Layer-3 multicast forwarding events.	debug ipv6 mrf event
Debugs the forwarding of IPv6 multi-layer multicast packets.	debug msf6 forwarding
Debugs the operation process of IPv6 multi-layer multicast forwarding entries.	debug msf6 mfc
Debugs the underlying hardware for IPv6 multi-layer multicast forwarding.	debug msf6 ssp
Debugs the APIs for IPv6 multi-layer multicast forwarding.	debug msf6 api
Debugs the processing of IPv6 multi-layer multicast forwarding events.	debug msf6 event

3. CONFIGURING IGMP

3.1 Overview

The Internet Group Management Protocol (IGMP) is a member of TCP/IP protocol family. It manages IP multicast members and is used to establish and maintain multicast group membership between hosts and directly neighboring multicast routers. IGMP behaviors are classified into host behaviors and device behaviors.

- At present, three IGMP versions are available, which are IGMPv1, IGMPv2 and IGMPv3.
- All IGMP versions support the Any-Source Multicast (ASM) model.
- IGMPv3 can be directly used for the Source-Specific Multicast (SSM) model.
- IGMPv1 and IGMPv2 can be used for the SSM model only when the IGMP SSM Mapping technology is supported.

Protocols and Standards

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

3.2 Applications

Application	Description
Local IGMP Service	Implements the IGMP service in a local network.
IGMP Proxy Service	In a simple tree network topology, use the IGMP proxy service instead of the PIM service.

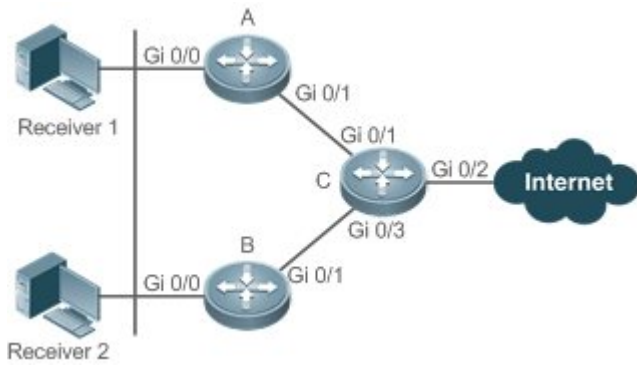
3.2.1 Local IGMP Service

Scenario

As shown in Figure 3-1, receivers 1 and 2 and routers A and B form a local network.

Query packets sent by router A or B are valid in the LAN, whereas Report packets sent by receivers 1 and 2 are also valid locally.

Figure 3-1



Remark	C is the egress gateway (EG) device.
s	A and B are core routers.

Deployment

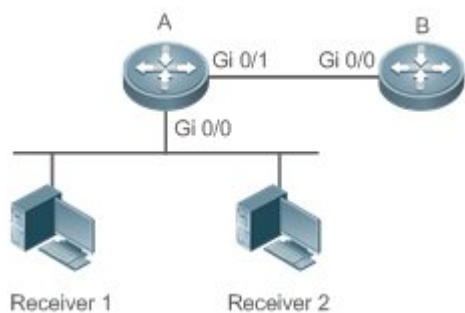
- Routers A, B and C run OSPF.
- The interfaces of A, B and C run multicast protocols (PIM-SM or PIM-DM).

3.2.2 IGMP Proxy Service

Scenario

As shown in Figure 3-2, router A implements the proxy function working as a host and forms a local network group with router B. Router A forwards Report packets sent by receivers 1 and 2.

Figure 3-2



Remark	Router A implements the proxy function.
s	Router B provides the PIM service.

Deployment

- Routers A and B run OSPF.
- The interfaces of A and B run multicast protocols (PIM-SM or PIM-DM).
- The multicast proxy function is implemented on the interfaces Gi0/0 and Gi0/1 of router A.

3.3 Features

Basic Concepts

- ❖ Host Behavior and Device Behavior
 - Layer-3 multicast devices that run multicast management protocols are called devices and their behaviors are called device behaviors.
 - PCs or simulated PCs that run multicast management protocols are called hosts and their behaviors are called host behaviors.
- ❖ Querier
 - Devices compete against each other by comparing IP addresses. Devices with lower IP addresses become queriers and send Query packets regularly.
- ❖ IGMP Proxy-Service Interface
 - This interface performs host behaviors, receives Query packets sent by upstream devices (hence also called uplink interface), and sends Report information collected by the router proxy.
- ❖ IGMP Mroute–Proxy Interface
 - This interface implements the router functions, sends packets received by the IGMP PROXY-SERVICE interface (hence also called downlink interface), and collects host information and sends the host information to the IGMP PROXY-SERVICE interface.
- ❖ IGMP SSM Mapping
 - Mapping of the SSM model. IGMPv1 and IGMPv2 do not support the SSM model, but can enable the SSM-MAP function to support the SSM model.

Overview

Feature	Description
IGMP Router	Sends Query packets and obtains local member information.
IGMP Querier	Selects a unique querier from a network segment.
IGMP Group Filtering	Filters group members and limit the number of group members.
Static IGMP Group	Static group information is available on a router; therefore, it is unnecessary for the host to send a Report packet to obtain the static group information.
Simulating Hosts to Join IGMP Groups	Simulate the host behavior to directly join a multicast group on an interface.
IGMP Proxy	Use this function in a simple tree network topology where no complex multicast route protocols (such as PIM) need to be executed.

Feature	Description
IGMP SSM Mapping	Provide the SSM model support for IGMPv1 and IGMPv2. When a host joins a group, you can specify a source to save bandwidth and prevent unwanted and invalid multicast data streams from occupying network bandwidth, especially in a network environment where multiple multicast sources share one multicast address.

3.3.1 IGMP Router

- This function is used to send Query packets and obtain local member information.

Working Principle

- A device regularly sends Query packets to make sure that at least one host is available in a group. When no host is available in the group, the device deletes this group.

Related Configuration

❖ Enabling IGMP

IGMP is disabled on an interface by default.

You can run the **ip pim { sparse-mode | dense-mode }** command to enable or disable IGMP for an interface.

IGMP can be enabled only when Sparse Mode (SM) or Dense Mode (DM) is configured on the interface.

❖ Specifying the IGMP Version

IGMPv2 is enabled by default.

You can run the **ip igmp version { 1 | 2 | 3 }** command to set or reset the IGMP version.

❖ Configuring the Last-Member Query Interval

The interval for sending the last-member Query packets is 1s by default.

You can run the **ip igmp last-member-query-interval interval** command to set or reset the interval for an interface to send Query packets.

A larger value means a larger interval; a smaller value means a smaller interval.

❖ Configuring the Last-Member Query Times

The number of the last-member query times is 2 by default.

You can run the **ip igmp last-member-query-count count** command to set or reset the number of the last-member query times.

A larger value means more last-member query times; a smaller value means fewer last-member query times.

❖ Configuring the Common Member Query Interval

The common member query interval is 125s by default.

You can run the **ip igmp query-interval** *seconds* command to set or reset the common member query interval.

A larger value means a larger common query interval; a smaller value means a smaller common query interval.

❖ Configuring the Maximum Response Time

The maximum response time is 10s by default.

You can run the **ip igmp query-max-response-time** *seconds* command to set or reset the maximum response time.

A larger value means longer response time; a smaller value means shorter response time.

3.3.2 IGMP Querier

Select a unique querier from a network segment. The querier sends Query packets to obtain group information of the local network.

Working Principle

In a multicast network running IGMP, a multicast device is specified for sending IGMP Query packets. This device is determined through selection. At the beginning, all devices are in the Querier state. When the devices receive membership queries from a device with a lower IP address, the devices change from the Querier state to the Non-querier state. Therefore, only one device is in the Querier state finally. This device has the lowest IP address among all multicast devices in the network. When the selected querier fails, IGMPv2 also works. Non-querier devices maintain the interval timer for survival of querier. This timer is reset each time a device receives a membership Query packet. If the timer expires, a new round of querier selection starts.

Related Configuration

❖ Configuring the Querier Timeout

The querier timeout is 255s by default.

You can run the **ip igmp query-timeout** *seconds* command to set the querier timeout.

A larger value means longer survival time; a smaller value means shorter survival time.

3.3.3 IGMP Group Filtering

Filter group members and limit the number of group members.

Working Principle

To prevent hosts in a network segment where an interface resides from joining a multicast group, you can configure an ACL on this interface as a filter. The interface will filter the received IGMP

membership Report packets based on this ACL, maintain group membership only for multicast groups allowed by this ACL and set the maximum number of router members.

Related Configuration

❖ Configuring the IGMP Group ACL

By default, no ACL is used and any group is allowed to join.

You can run the **ip igmp access-group** *access-list-name* command to set or reset the multicast group ACL.

After the ACL is configured, a router receives only packets set in the ACL.

❖ Configuring the Maximum Number of IGMP Group Members

The maximum number of IGMP group members is 1,024 by default.

You can run the **ip igmp limit** *number* command to set or reset the maximum number of multicast group members.

A larger value means more members; a smaller value means fewer members.

3.3.4 Static IGMP Group

When static IGMP groups are available on a router, it is unnecessary for the host to send a Report packet to obtain the static group information. The router can directly exchange group information with a PIM router.

Working Principle

You need to set static group information manually.

Related Configuration

❖ Configuring a Static Group

No static group is configured by default.

You can run the **ip igmp static-group** *group-address* command to configure a static group.

3.3.5 Simulating Hosts to Join IGMP Groups

Simulate the host behavior to directly join a multicast group on an interface.

Related Configuration

❖ Configuring the Join-Group function

No join-group information is set by default.

You can run the **ip igmp join-group** *group-address* command to configure the address of the multicast group to be joined by the simulated host.

3.3.6 IGMP Proxy

Use this function in a simple tree network topology where no complex multicast route protocols (such as PIM) need to be executed. In this way, a downstream proxy host can send IGMP packets and maintain the membership.

Working Principle

When an upstream router is configured as an IGMP proxy-service interface, it is equal to a host that can receive Query packets sent by upstream routers or forward group information sent by downstream hosts. When a downstream router is configured as an IGMP multicast proxy interface, it is equal to a router that can forward Query packets sent by upstream routers or receive Report packets sent by downstream routers.

Related Configuration

❖ Configuring the IGMP Proxy Service

The IGMP proxy service function is disabled by default.

You can run the **ip igmp proxy-service** command to enable the IGMP proxy service.

This function is mandatory when a proxy is to be used.

❖ Configuring the IGMP Mroute Proxy

The IGMP mroute proxy function is disabled by default.

You can run the **ip igmp mroute-proxy *interfacename*** command to enable the IGMP mroute proxy.

This function is mandatory when a proxy is to be used.

3.3.7 IGMP SSM Mapping

Provide the SSM model support for IGMPv1 and IGMPv2. When a host joins a group, you can specify a source to save bandwidth and prevent unwanted and invalid multicast data streams from occupying network bandwidth, especially in a network environment where multiple multicast sources share one multicast address.

Working Principle

Based on IGMP v1/v2, IGMPv3 provides an extra function, namely, the multicast source filter function. In IGMPv1/v2, a host determines to join a group only based on the group address and then receive multicast streams sent to this group address from any source. A host using IGMPv3 advertises the multicast group that the host wants to join and the addresses of multicast sources from which this host wants to receive packets. IGMPv1 and IGMPv2 also implement "source address filtering" in some sense; however, they implement this function on the multicast receivers by enabling the SSM mapping function and configuring the static SSM mapping group.

Related Configuration

❖ Enabling IGMP SSM Mapping

The SSM mapping function is disabled by default.

You can run the **ip igmp ssm-map enable** command to enable the function.

Mandatory.

❖ Configuring Static IGMP SSM Mapping

No static SSM mapping is set by default.

You can run the **ip igmp ssm-map static access-list-num A.B.C.D** command to configure static SSM mapping.

3.4 Configuration

Configuration	Description and Command	
Configuring IGMP Basic Functions	(Mandatory) It is used to set up the multicast service.	
	ip multicast-routing	Enables the IPv4 multicast routing function.
	ip pim { sparse-mode dense-mode }	Enables the PIM-SM or PIM-DM function.
Configuring IGMP Routers	ip igmp version { 1 2 3 }	Specifies the IGMP version.
	ip igmp last-member-query-interval interval	Configures the last-member query interval.
	ip igmp last-member-query-count count	Configures the last-member query times.
	ip igmp query-interval seconds	Configures the membership query interval.
Configuring IGMP Querier	ip igmp query-max-response-time seconds	Configures the maximum response time.
	ip igmp query-timeout seconds	Configures the querier timeout.
Configuring IGMP Group Filtering	ip igmp access-group access-list	Configures the IGMP group ACL.
	ip igmp limit number [except access-list]	Configures the maximum number of IGMP group members.
Configuring IGMP Proxy	ip igmp proxy-service	Configures the IGMP proxy service.
	ip igmp mroute-proxy interface-type interface-number	Configures the IGMP mroute proxy.
Configuring IGMP SSM Mapping	ip igmp ssm-map enable	Enables IGMP SSM mapping.
	ip igmp ssm-map static access-list source-address	Configures static IGMP SSM mapping.

3.4.1 Configuring IGMP Basic Functions

Configuration Effect

- Enable the multicast routing function of a local network and collect group information of the local network.

Notes

- An interface must be enabled with the PIM-SM or PIM-DM function.

Configuration Steps

❖ Enabling the IPv4 Multicast Routing Function

- Mandatory.
- If there is no special requirement, the IPv4 multicast routing function should be enabled on each router in the local network.

❖ Enabling the PIM-SM or PIM-DM Function

- Mandatory.
- If there is no special requirement, the PIM-SM or PIM-DM function should be directly enabled on an interface of the local network.

Verification

Run the **show ip igmp interface** *interface-type interface-number* command to check whether IGMP is enabled on the interface.

Related Commands

❖ Enabling the IPv4 Multicast Routing Function

Command	ip multicast-routing
Parameter	N/A
Description	
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Enabling the PIM-SM or PIM-DM Function

Command	ip pim { sparse-mode dense-mode }
Parameter	N/A
Description	
Command Mode	Interface configuration mode
Usage Guide	PIM interfaces must be layer-3 interfaces, including routing interfaces, L3AP, SVI and loopback interfaces. All PIM interfaces should be accessible to IPv4 unicast routes.

Configuration Example

❖ Enabling IGMP for a Local Network

Scenario	<ul style="list-style-type: none"> ➤ Configure an IPv4 unicast routing protocol (such as OSPF) on a router and ensure that the loopback interface is accessible to a unicast route. ➤ Enable the IPv4 multicast route function on all routers. ➤ Enable the PIM-SM or PIM-DM function on interfaces interconnecting devices and interfaces connecting user hosts and multicast sources.
	<pre>VSU(config)#ip multicast routing VSU(config)#int gi 0/5 VSU(config if GigabitEthernet 0/5)#ip add 192.168.1.90 255.255.255.0 VSU(config if GigabitEthernet 0/5)#ip pim sparse mode</pre>
Verification	Run the show ip igmp interface <i>interface-type interface-number</i> command to check whether IGMP is enabled on the interface.
	<pre>VSU#show ip igmp interface gigabitEthernet 0/5 Interface GigabitEthernet 0/5 (Index 5) IGMP Active, Querier, Version 2 (default) Internet address is 192.168.1.90 IGMP interface limit is 1024 IGMP interface has 1 group record states IGMP interface has 0 static group records IGMP activity: 3 joins, 0 leaves 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 10 Last member query count is 2 Group Membership interval is 260 seconds Robustness Variable is 2</pre>

Common Errors

- Routers in the network are not enabled with the multicast routing function.
- No multicast interface is available in the network.

3.4.2 Configuring IGMP Routers**Configuration Effect**

- Modify the IGMP router parameters will affect the type of packets to be sent and the sending method.

Notes

- The basic functions of IGMP must be configured.

Configuration Steps

- ❖ Specifying the IGMP Version

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

- ❖ Configuring the Last-Member Query Interval

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

- ❖ Configuring the Last-Member Query Times

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

- ❖ Configuring the Common Member Query Interval

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

- ❖ Configuring the Maximum Response Time

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

Verification

Run the **show ip igmp interface** *interface-type interface-number* command to display the interface configurations.

Related Commands

- ❖ Specifying the IGMP Version

Command	ip igmp version { 1 2 3 }
---------	-------------------------------

Parameter	1: Indicates IGMPv 1.
Description	2: Indicates IGMPv 2. 3: Indicates IGMPv 3.
Command	Interface configuration mode
Mode	
Usage Guide	After this command is configured, IGMP will automatically restart.

❖ Configuring the Last-Member Query Interval

Command	ip igmp last-member-query-interval <i>interval</i>
Parameter	<i>Interval</i> : Indicates the interval for sending the Query packets of a specific group. The value ranges from 1 to 255 in the unit of 0.1s, and the default value is 10 (namely, 1s).
Description	
Command	Interface configuration mode
Mode	
Usage Guide	This command applies only to IGMPv2 or IGMPv3. When an interface receives a Leave packet, the interface sends Query packets of the group continually and waits for a response from the host. After timeout occurs, the IGMP router assumes that the group member does not exist in the directly connected network segment and deletes the interface from the IGMP group. The timeout duration is equal to the value of last-member-query-interval multiplied by last-member-query-count plus 1/2 of query-max-response-time .

❖ Configuring the Last-Member Query Times

Command	ip igmp last-member-query-count <i>count</i>
Parameter	<i>count</i> : Indicates the times for sending the Query packets of a specific group, ranging from 2 to 7. The default value is 2.
Description	
Command	Interface configuration mode
Mode	
Usage Guide	This command applies only to IGMPv2 or IGMPv3. When an interface receives a Leave packet, the interface sends Query packets of the group continually and waits for a response from the host. After timeout occurs, the IGMP router assumes that the group member does not exist in the directly connected network segment and deletes the interface from the IGMP group. The timeout duration is equal to the value of last-member-query-interval multiplied by last-member-query-count plus 1/2 of query-max-response-time .

❖ Configuring the Common Member Query Interval

Command	ip igmp query-interval <i>seconds</i>
Parameter	<i>seconds</i> : Indicates the common member query interval, ranging from 1 to 18,000s. The default value is 125.
Description	
Command	Interface configuration mode
Mode	
Usage Guide	N/A

❖ Configuring the Maximum Response Time

Command	ip igmp query-max-response-time <i>seconds</i>
----------------	---

Parameter Description	<i>seconds</i> : Indicates the maximum response time, ranging from 1 to 25s. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	After sending Query packets, the interface waits for a response. If timeout occurs, the IGMP router assumes that the group member does not exist in the directly connected network segment and deletes the group information.

Configuration Example

❖ Configuring Basic Router Parameters

Scenario	<ul style="list-style-type: none"> ➤ Configure basic functions of IGMP. ➤ Specify the IGMPv3. ➤ Configure the last-member query interval to 15 (1.5s). ➤ Configure the number of the last-member queries to 3. ➤ Configure the common member query interval to 130s. ➤ Configure the maximum response time to 15s.
	<pre>VSU(config if GigabitEthernet 0/5)#ip igmp version 3 VSU(config if GigabitEthernet 0/5)#ip igmp last member query count 3 VSU(config if GigabitEthernet 0/5)#ip igmp last member query interval 15 VSU(config if GigabitEthernet 0/5)#ip igmp query interval 130 VSU(config if GigabitEthernet 0/5)#ip igmp query max response time 15</pre>
Verification	Run the show ip igmp interface <i>interface-type interface-number</i> command to check the IGMP functions of the interface.
	<pre>VSU#show ip igmp interface gigabitEthernet 0/5 Interface GigabitEthernet 0/5 (Index 5) IGMP Enabled, Active, Querier, Version 3 Internet address is 192.168.1.90 IGMP interface limit is 1024 IGMP interface has 1 group record states IGMP interface has 0 static group records IGMP activity: 3 joins, 0 leaves IGMP query interval is 130 seconds IGMP querier timeout is 267 seconds IGMP max query response time is 15 seconds</pre>

Scenario	<ul style="list-style-type: none"> ➤ Configure basic functions of IGMP. ➤ Specify the IGMPv3. ➤ Configure the last-member query interval to 15 (1.5s). ➤ Configure the number of the last-member queries to 3. ➤ Configure the common member query interval to 130s. ➤ Configure the maximum response time to 15s.
	<pre>VSU(config if GigabitEthernet 0/5)#ip igmp version 3 VSU(config if GigabitEthernet 0/5)#ip igmp last member query count 3 VSU(config if GigabitEthernet 0/5)#ip igmp last member query interval 15 VSU(config if GigabitEthernet 0/5)#ip igmp query interval 130 VSU(config if GigabitEthernet 0/5)#ip igmp query max response time 15</pre>
	<pre>Last member query response interval is 15 Last member query count is 3 Group Membership interval is 275 seconds Robustness Variable is 2 VSU#</pre>

Common Errors

- The basic functions of IGMP are not enabled.

3.4.3 Configuring IGMP Querier

Configuration Effect

- Select a unique querier in a local network.

Notes

- The basic functions of IGMP must be configured.

Configuration Steps

- If necessary, the querier timeout can be configured.
- If there is no special requirement, you can perform the configuration on all interfaces enabled with IGMP in the local network.

Verification

Run the **show ip igmp interface *interface-type interface-number*** command to display the interface configurations.

Related Commands

❖ Configuring the Querier Timeout

Command	ip igmp query-timeout <i>seconds</i>
Parameter Description	<i>seconds</i> : Indicates the keepalive time of the querier, ranging from 60 to 300s. The default value is 255s.
Command Mode	Interface configuration mode
Usage Guide	After sending Query packets, an interface waits for Query packets sent by other devices. If timeout occurs, the IGMP router assumes that the querier is unique in the directly connected network segment.

Configuration Example

❖ Configuring the Querier Timeout

Scenario	<ul style="list-style-type: none"> ➤ Configure basic functions of IGMP. ➤ Set the querier timeout to 280S.
	<pre>VSU(config-if GigabitEthernet 0/5)#ip igmp query timeout 280</pre>
Verification	Run the show ip igmp interface <i>interface-type interface-number</i> command to check the IGMP functions of the interface.
	<pre>VSU#show ip igmp interface gigabitEthernet 0/5 Interface GigabitEthernet 0/5 (Index 5) IGMP Enabled, Active, Querier, Version 3 Internet address is 192.168.1.90 IGMP interface limit is 1024 IGMP interface has 1 group record states IGMP interface has 0 static group records IGMP activity: 11 joins, 0 leaves IGMP query interval is 130 seconds IGMP querier timeout is 280 seconds IGMP max query response time is 15 seconds Last member query response interval is 15 Last member query count is 3 Group Membership interval is 275 seconds Robustness Variable is 2 VSU#</pre>

Common Errors

- The basic functions of IGMP are not enabled.

3.4.4 Configuring IGMP Group Filtering

Configuration Effect

- A router filters IGMP group members.

Notes

- The basic functions of IGMP must be configured.

Configuration Steps

- ❖ Configuring the IGMP Group ACL

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

- ❖ Configuring the Maximum Number of IGMP Group Members

Optional.

If there is no special requirement, you can perform this configuration on all router interfaces directly connected to the local network.

Verification

- ❖ IGMP Group ACL

- Configure an interface to allow only groups in ACL 1 to join. The access addresses of ACL 1 are 225.0.0.1~225.0.0.255.
- Configure the interface to join a group whose address is 225.0.0.5.
- Configure the interface to join a group whose address is 236.0.0.5.
- View the group information of the current interface.

- ❖ Maximum Number of IGMP Group Members

- Set the maximum member quantity to 5 on an interface.
- Configure the interface to join a group whose address is from 225.0.0.5 to 225.0.0.10.
- View the group information of the interface.

Related Commands

- ❖ Configuring the IGMP Group ACL

Command
<code>ip igmp access-group <i>access-list</i></code>

Parameter Description	<i>access-list</i> : Defines a group address range by using a standard IP ACL or an extended ACL. The value ranges from 1 to 199, 1300 to 2699 and characters.
Command Mode	Interface configuration mode
Usage Guide	<p>Configure this command on an interface to control the groups that hosts in a directly connected network segment can join. Use an ACL to limit the group address range. If Report packets denied by the ACL are received, the packets will be discarded.</p> <p>When IGMPv3 is enabled, this command supports an extended ACL. If the received IGMP Report information is (S1,S2,S3...Sn,G), this command will apply the corresponding ACL to the (0,G) information for matching. Therefore, you must configure a (0,G) record explicitly for the extended ACL in order to normally filter (S1,S2,S3...Sn,G).</p>

❖ Configuring the Maximum Number of IGMP Group Members

Command	ip igmp limit <i>number</i> [except <i>access-list</i>]
Parameter Description	<p><i>number</i>: Indicates the maximum number of IGMP group members, whose value range varies with devices. The default value is 1,024 for an interface and 65,536 globally.</p> <p>except <i>access-list</i>: Indicates that the groups in the ACL are not counted.</p> <p>access-list indicates a standard IP ACL. The value ranges from 1 to 99, 1300 to 1999 and words.</p>
Command Mode	Interface configuration mode
Usage Guide	<p>Global configuration mode: Limits the maximum quantity of the IGMP group members in a system.</p> <p>Interface configuration mode: limits the maximum quantity of IGMP group members on an interface. If the quantity of group members exceeds the interface or global limit, the Report packets received subsequently will be ignored.</p> <p>If an Except ACL is configured, Report packets within a specified range can be normally processed; therefore, the generated group members are not counted.</p> <p>The interface and global configurations can be performed independently. If the global quantity limit is smaller than that for an interface, the global configuration shall be used.</p>

Configuration Example

❖ Configuring IGMP Group Filtering

Scenario	<ul style="list-style-type: none"> ➤ Configure the basic functions of IGMP. ➤ Configure the access address range of ACL 1 from 225.0.0.1 to 225.0.0.255. ➤ Set the address of the group to be joined to 225.0.0.5. ➤ Set the address of the group to be joined to 236.0.0.5.
	<pre>VSU(config)#access list 1 permit 225.0.0.1 225.0.0.255 VSU(config if GigabitEthernet 0/5)#ip igmp access group 1 VSU(config if GigabitEthernet 0/5)#ip igmp join group 225.0.0.5 VSU(config if GigabitEthernet 0/5)#ip igmp join group 236.0.0.5</pre>
Verification	Run the show ip igmp groups [<i>interface-type interface-number</i>] [<i>group-address</i>] [detail] command to display the group information of the interface.

```

VSU(config if GigabitEthernet 0/5)#show ip igmp groups
IGMP Connected Group Membership
Group Address      Interface                Uptime    Expires    Last
Reporter
225.0.0.5          GigabitEthernet 0/5     00:14:00  00:02:45
192.168.1.90

```

❖ Configuring the Maximum Number of IGMP Group Members

Scenario	<ul style="list-style-type: none"> ➤ Configure the basic functions of IGMP. ➤ Configure the maximum number of IGMP group members for the interface to 5. ➤ Add group information (225.0.0.5~225.0.0.12). ➤ View group information.
	<pre> VSU(config if GigabitEthernet 0/5)#ip igmp limit 5 VSU(config if GigabitEthernet 0/5)# VSU(config if GigabitEthernet 0/5)#ip igmp join group 225.0.0.5 VSU(config if GigabitEthernet 0/5)#ip igmp join group 225.0.0.6 VSU(config if GigabitEthernet 0/5)#ip igmp join group 225.0.0.7 VSU(config if GigabitEthernet 0/5)#ip igmp join group 225.0.0.8 VSU(config if GigabitEthernet 0/5)#ip igmp join group 225.0.0.9 VSU(config if GigabitEthernet 0/5)#ip igmp join group 225.0.0.10 VSU(config if GigabitEthernet 0/5)#ip igmp join group 225.0.0.11 VSU(config if GigabitEthernet 0/5)#ip igmp join group 225.0.0.12 </pre>
Verification	<p>Run the show ip igmp groups [<i>interface-type interface-number</i>] [<i>group-address</i>] [<i>detail</i>] command to display the group information of the interface.</p>
	<pre> VSU(config if GigabitEthernet 0/5)#show ip igmp groups IGMP Connected Group Membership Group Address Interface Uptime Expires Last Reporter 225.0.0.5 GigabitEthernet 0/5 00:20:15 00:03:09 192.168.1.90 225.0.0.6 GigabitEthernet 0/5 00:20:24 00:02:58 192.168.1.90 225.0.0.7 GigabitEthernet 0/5 00:00:15 00:04:29 192.168.1.90 </pre>

225.0.0.8	GigabitEthernet 0/5	00:00:13	00:04:34
192.168.1.90			
225.0.0.9	GigabitEthernet 0/5	00:00:11	00:04:33
192.168.1.90			

Common Errors

- The basic functions of IGMP are not enabled.

3.4.5 Configuring IGMP Proxy

Configuration Effect

- Configure the router proxy function and collect local member information.

Notes

- The basic functions of IGMP must be configured.

Configuration Steps

❖ Configuring the IGMP Proxy Service

- Optional.
- If there is no special requirement, you can perform this configuration on directly connected upstream router interfaces.

❖ Configuring the IGMP Mroute Proxy

- Optional.
- If there is no special requirement, you can perform this configuration on directly connected downstream host interfaces.

Verification

- Set interface 7 for directly connecting to an upstream router as a multicast proxy server.
- Set interface 1 for directly connecting to a downstream host as a multicast proxy.
- Set interface 1 to be joined by groups whose addresses are 225.0.0.6 and 225.5.5.5.
- View the current group information.

Related Commands

❖ Configuring the IGMP Proxy Service

Command	<code>ip igmp proxy-service</code>
Parameter	N/A
Description	
Command Mode	Interface configuration mode
Usage Guide	Run the <code>ip igmp proxy-service</code> command to set the uplink interface as a Proxy-Service interface.

	<p>Run the ip igmp mroute-proxy command to set the downlink interface as a Mroute-Proxy interface.</p> <p>Forward IGMP Query packets from the Proxy-Service interface to the Mroute-Proxy interface.</p> <p>Forward IGMP Report packets from the Mroute-Proxy interface to the Proxy-Service interface.</p> <p>A device allows a maximum of 32 Proxy-Service interfaces. After a Proxy-Service interface receives an IGMP Query packet, the interface sends a response based on the IGMP group member records.</p> <p>If the switchport command is executed on the Proxy-Service interface, the ip igmp mroute-proxy command configured on the Mroute-Proxy interface will be deleted automatically.</p>
--	---

❖ Configuring the IGMP Mroute Proxy

Command	ip igmp mroute-proxy <i>interface-type interface-number</i>
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	<p>Run the ip igmp proxy-service command to set the uplink interface as a Proxy-Service interface.</p> <p>Run the ip igmp mroute-proxy command to set the downlink interface as a Mroute-Proxy interface.</p> <p>Forward IGMP Query packets from the Proxy-Service interface to the Mroute-Proxy interface.</p> <p>Forward IGMP Report packets from the Mroute-Proxy interface to the Proxy-Service interface.</p>

Configuration Example

Scenario	<ul style="list-style-type: none"> ➤ Configure basic functions of IGMP. ➤ Configure interface 7 as a proxy server. ➤ Configure interface 1 as a multicast proxy. ➤ Set interface 1 to be joined by groups whose addresses are 225.0.0.6 and 225.5.5.5.
	<pre>VSU(config if GigabitEthernet 0/7)#ip igmp proxy service VSU(config if GigabitEthernet 0/7)#exit VSU(config)#int gi 0/1 VSU(config if GigabitEthernet 0/1)#ip igmp mroute proxy gigabitEthernet 0/7 VSU(config if GigabitEthernet 0/1)#ip igmp join group 225.0.0.6 VSU(config if GigabitEthernet 0/1)#ip igmp join group 225.5.5.5</pre>
Verification	<p>Run the show ip igmp groups [<i>interface-type interface-number</i>] [<i>group-address</i>] [<i>detail</i>] command to display the group information of the interface.</p>
	<pre>VSU(config if GigabitEthernet 0/1)#show ip igmp groups IGMP Connected Group Membership Group Address Interface Uptime Expires Last Reporter</pre>

```

225.0.0.6      GigabitEthernet 0/1    00:23:05  00:02:40
192.168.36.90
225.5.5.5     GigabitEthernet 0/1    00:22:06  00:02:41
192.168.36.90

IGMP Proxy server Connected Group Membership
Group Address      Interface          Uptime
225.0.0.6         GigabitEthernet 0/7    00:23:05
225.5.5.5         GigabitEthernet 0/7    00:22:06

VSU(config if GigabitEthernet 0/1)#

```

Common Errors

- The basic functions of IGMP are not enabled.

3.4.6 Configuring IGMP SSM Mapping

Configuration Effect

- IGMPv3 supports source filtering; however, IGMPv1 and IGMPv2 do not support source filtering, but provides the SSM mapping function to filter sources.

Notes

- The basic functions of IGMP must be configured.

Configuration Steps

- ❖ Enabling SSM Mapping

(Mandatory) Enable the SSM mapping function.

Enable the SSM mapping function on a router.

- ❖ Configuring Static SSM Mapping

Optional.

Configure this function on routers enabled with SSM mapping.

Verification

Run the **show ip igmp ssm-mapping [group-address]** command to display SSM mapping information.

Related Commands

- ❖ Enabling SSM Mapping

Command	ip igmp ssm-map enable
Parameter	N/A
Description	
Command Mode	Global configuration mode
Usage Guide	Run the ip igmp ssm-map enable command to enable the SSM mapping function. Run the ip igmp ssm-map static command to set static mapping entries. Run IGMPv3 on the interface. When IGMPv1 or IGMPv2 Report packets are received, source addresses of static mappings can be added.

❖ Configuring Static SSM Mapping

Command	ip igmp ssm-map static <i>access-list source-address</i>
Parameter Description	<i>N/A</i> <i>access-list</i> : Indicates the group address range set by a standard IP ACL. The value ranges from 1 to 99, 1300 to 1999 and words. <i>source-address</i> : Indicates the source address.
Command Mode	Global configuration mode
Usage Guide	Run the ip igmp ssm-map enable command to enable the SSM mapping function. Run the ip igmp ssm-map static command to set static mapping entries. Run IGMPv3 on the interface. When IGMPv1 or IGMPv2 Report packets are received, source addresses of static mappings can be added.

Configuration Example

Scenario	<ul style="list-style-type: none"> ➤ Configure the basic functions of IGMP. ➤ Enable SSM mapping. ➤ Configure static SSM mapping ACL 1.
	<pre>VSU(config)#ip igmp ssm map enable VSU(config)#ip igmp ssm map static 1 192.168.5.9</pre>
Verification	Run the show ip igmp ssm-mapping [group-address] command to display SSM mapping information.
	<pre>VSU#show ip igmp ssm mapping SSM Mapping : Enabled Database : Static mappings configured</pre>

Common Errors

- The basic functions of IGMP are not enabled.

3.5 Monitoring

Clearing

Description	Command
Clears dynamic group membership from the IGMP buffer.	clear ip igmp group
Clears interface information from the IGMP buffer.	clear ip igmp interface <i>interface-type interface-number</i>

Displaying

Description	Command
Displays all groups in a directly connected subnet.	show ip igmp groups
Displays details about all groups in a directly connected subnet.	show ip igmp groups detail
Displays specified groups in a directly connected subnet.	show ip igmp groups <i>A.B.C.D</i>
Displays details about specified groups in a directly connected subnet.	show ip igmp groups <i>A.B.C.D detail</i>
Displays IGMP configurations of a specified interface in a directly connected subnet.	show ip igmp interface <i>interface-type interface-number</i>
Displays details about all groups of a specified interface in a directly connected subnet.	show ip igmp groups <i>interface-type interface-number detail</i>
Displays information about a specified group of a specified interface in a directly connected subnet.	show ip igmp groups <i>interface-type interface-number A.B.C.D</i>
Displays details about a specified group of a specified interface in a directly connected subnet.	show ip igmp groups <i>interface-type interface-number A.B.C.D detail</i>
Displays configurations of an IGMP interface.	show ip igmp interface [<i>interface-type interface-number</i>]
Displays configurations of all IGMP interfaces.	show ip igmp interface
Displays configurations of IGMP SSM mapping.	show ip igmp ssm-mapping
Displays the information of IGMP SSM mapping to <i>A.B.C.D</i> .	show ip igmp ssm-mapping <i>A.B.C.D</i>

Debugging

Description	Command
Displays whether IGMP debugging is enabled.	show debugging

Description	Command
Debugs all IGMP information.	debug ip igmp all
Debugs IGMP packet decoding.	debug ip igmp decode
Debugs IGMP packet encoding.	debug ip igmp encode
Debugs IGMP events.	debug ip igmp events
Debugs IGMP FSM.	debug ip igmp fsm
Debugs IGMP state machine.	debug ip igmp tib
Debugs IGMP warning.	debug ip igmp warning

4. CONFIGURING MLD

4.1 Overview

Multicast Listener Discovery (MLD) is a protocol used in the multicast technology.

This protocol receives the multicast member relationship between hosts and routers to determine multicast flow forwarding. Using information obtained from MLD, a device maintains an interface-based multicast listener status table. The multicast listener status table is activated only when at least one host in the link of the interface is a group member.

Currently, MLD has two versions: MLDv1 and MLDv2.

- MLD of both versions supports the Any-Source Multicast (ASM) model.
- MLDv2 can be directly applied to the Source-Specific Multicast (SSM) model.
- MLDv1 can be applied to the SSM model only when MLD SSM mapping is configured.

Protocols and Standards

- RFC2710: Multicast Listener Discovery (MLDv1) for IPv6
- RFC3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6

4.2 Applications

Application	Description
Configuring the MLD Service on the Local Network	Implements the MLD service on the local network.
Configuring the MLD Proxy Service	In the simple tree topology, the MLD proxy service, instead of the PIM service, is used.

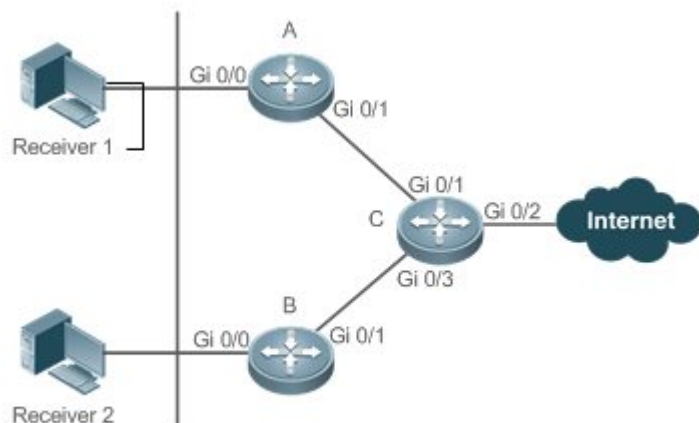
4.2.1 Configuring the MLD Service on the Local Network

Scenario

As shown in Figure 4-1, the local network consists of receiver 1, receiver 2, router A, and router B.

Query messages sent by router A or router B are valid on the local network, and Report messages sent by receiver A and receiver B are also valid on the local network.

Figure 4-1



Remark	Router C is the egress gateway.
s	Routers A and B are local routers.

Deployment

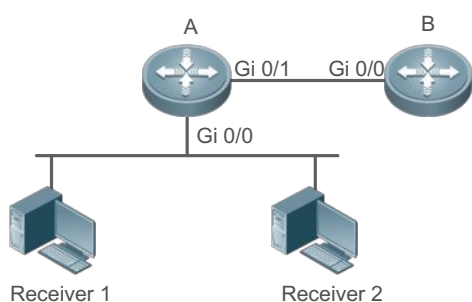
- Routers A, B, and C run the OSPFv6 protocol.
- Interfaces on routers A, B, and C run the multicast protocol (PIM SMv6).

4.2.2 Configuring the MLD Proxy Service

Scenario

As shown Figure 4-2, the proxy function is enabled on router A. Router A functions as a host and forms a local management group with router B. Router A forwards Report messages from receivers 1 and 2.

Figure 4-2



Remark	Router A functions as the proxy.
s	Router B provides the PIM service.

Deployment

- Routers A and B run the OSPFv6 protocol.
- Interfaces on routers A and B run the multicast protocol (PIM SMv6).

- The multicast proxy service is enabled on Gi 0/0 and Gi 0/1 of router A.

4.3 Features

Basic Concepts

❖ Host Behaviors and Device Behaviors

Layer-3 multicast devices running multicast management protocols are referred to as devices and their behaviors are device behaviors.

PCs or simulated PCs running multicast management protocols are referred to as hosts and their behaviors are host behaviors.

❖ Querier

Devices interact and compete with each other. After IP address comparison, the device with a lower IP address becomes the querier and periodically sends Query messages.

❖ MLD PROXY-SERVICE Interface

This interface, also called uplink interface, implements host behaviors. It receives Query messages sent by upstream devices and sends Report messages collected by the router proxy.

❖ MLD MROUTE PROXY Interface

This interface, also called downlink interface, implements router functions. It sends messages received by the proxy service interface and collects and sends host information to the proxy service interface.

❖ MLD SSM-MAP

SSM mapping refers to mapping of source-specific multicast. MLDv1 does not support the SSM model until the SSM-MAP function is enabled.

Overview

Feature	Description
Setting MLD Router Parameters	Sends Query messages to obtain local member information.
Querier Selection Process or Timeout Mechanism	Selects the unique querier in the current network segment.
Filtering MLD Groups	Filters group members and limits the number of group members.
Supporting Static MLD Groups	Stores static group information on the local router instead of obtaining group information by sending Report messages.

Feature	Description
Configuring Simulated Host Group Information	Simulates host behaviors to directly configure group joining information.
Supporting MLD Proxy	Uses this function in the simple tree topology instead of complex multicast routing protocols, such as the PIM.
Supporting SSM-MAP	Provides the SSM model for MLDv1. When a host is added to a group, a specific source can be specified to avoid network bandwidth occupation by unnecessary and invalid multicast data streams. This function is especially useful on a network where multiple multicast sources share the same multicast address.

4.3.1 Setting MLD Router Parameters

Sends Query messages to obtain local member information.

Working Principle

A device periodically sends Query messages to ensure that a group has at least one host. If no host is available in a group, the group will be deleted.

Related Configuration

❖ Enabling MLD

By default, MLD is disabled on an interface.

Run the **ipv6 pim { sparse-mode }** command to enable or disable MLD on an interface.

MLD can be enabled only after PIM SM is enabled on the interface.

❖ Configuring MLD Version

By default, the MLD version is 2.

Run the **ipv6 mld version { 1 | 2 }** command to configure or restore the MLD version of an interface.

❖ Configuring the Query Interval of the Last Member

By default, the interval for sending Query messages is 1s.

Run the **ipv6 mld last-member-query-interval *interval*** command to configure or restore the interval for sending Query messages.

A larger value means a longer interval for sending Query messages.

❖ Configuring the Number of Times for Querying the Last Member

By default, the number of times for querying the last member is 2.

Run the **ipv6 mld last-member-query-count *count*** command to configure or restore the number of times for querying the last member.

A larger value means a larger number of times for querying the last member.

❖ Configuring the Interval for Querying a Common Member

By default, the interval for querying a common member is 125s.

Run the **ipv6 mld query-interval** *seconds* command to configure or restore the interval for querying a common member.

A larger value means a longer interval for querying a common member.

❖ Configuring the Maximum Response Time

By default, the maximum response time is 10s.

Run the **ipv6 mld query-max-response-time** *seconds* command to configure or restore the maximum response time.

A larger value means a longer maximum response time.

4. 3. 2 Querier Selection Process or Timeout Mechanism

Selects the unique querier in the current network segment. The querier sends a Query message to obtain group information on the local network.

Working Principle

On a multicast network running MLD, a multicast device dedicated to query sends MLD Query messages. The device is determined by election. Initially, all devices are in the querier state. When receiving member relationship Query messages from devices with lower IP addresses, the devices switch from the receiver state to non-querier state. Therefore, there is only one device in the query state in the end. This device has the lowest IP address among all multicast devices on the network. When the querier device does not work, MLD also works. Non-querier devices maintain the keepalive interval timer for other queriers. The timer is reset once the device receives a member relationship query message. If the timer times out, the device starts to send Query messages and a new querier election starts.

Related Configuration

❖ Configuring the Keepalive Interval of the Querier

By default, the keepalive interval of the querier is 255s.

Run the **ipv6 mld querier-timeout** *seconds* command to configure or restore the keepalive interval of the querier.

A larger value means a longer keepalive interval of the querier.

4. 3. 3 Filtering MLD Groups

Filters group members and limits the number of group members.

Working Principle

If you do not want hosts in the network segment where an interface resides to be added to certain multicast groups, you can configure ACL rules on the interface as a filter. The interface will filter received MLD member relationship Report messages based on the ACL rules and maintain member relationships only for multicast groups permitted by the rules. The largest number of router members can also be set.

Related Configuration

❖ Configuring Access Control for Multicast Groups

By default, no access control is configured and hosts can be added to any groups.

Run the **ipv6 mld access-group** *access-list-name* command to configure or restore access control for multicast groups.

After the configuration, the router can receive messages only from hosts in groups specified in the access list.

❖ Configuring the Maximum Number of MLD Group Members

By default, an MLD group has a maximum of 1024 members.

Run the **ipv6 mld limit** *number* command to configure or restore the maximum number of MLD group members.

A larger value means a larger number of group members.

4.3.4 Supporting Static MLD Groups

Stores static group information on a local router instead of obtaining group information by sending Report messages. The local router can directly exchange group information with the PIM router.

Working Principle

Manually configure static group information.

Related Configuration

❖ Configuring Static-Group

By default, no static group information is configured.

Run the **ipv6 mld static-group** *group-address* command to configure or cancel static group information.

4.3.5 Configuring Simulated Host Group Information

Simulates host behaviors to directly configure group joining information.

Related Configuration

❖ Configuring Join-Group

By default, no join-group information is configured.

Run the **ipv6 mld join-group** *group-address* command to configure or cancel join-group information.

4.3.6 Supporting MLD Proxy

In the simple tree topology, it is not necessary to run complex multicast routing protocols (such as PIM). In this case, MLD proxy can be used to send MLD messages for downstream hosts and maintain member relationships.

Working Principle

When an upstream router is configured as an MLD proxy service interface, it functions as a host and can receive Query messages from upstream routers as well as forward group information of downstream hosts. When a downstream router is configured as an MLD multicast proxy interface, it functions as a router and can forward Query messages of upstream routers as well as receive Report messages from downstream routers.

Related Configuration

❖ Configuring MLD PROXY-SERVICE

By default, the MLD proxy service is disabled on an interface.

Run the **ipv6 mld proxy-service** command to configure or cancel the MLD proxy function on an interface.

This function must be configured when proxy is used.

❖ Configuring MLD MROUTE-PROXY

By default, the multicast proxy service is disabled on an interface.

Run the **ipv6 mld mroute-proxy** *interfacename* command to configure or cancel the multicast proxy function on an interface.

This function must be configured when proxy is used.

4.3.7 Supporting SSM-MAP

This function provides the SSM model for MLDv1. When a host is added to a group, a specific source can be specified to avoid network bandwidth occupation by unnecessary and invalid multicast data streams. This function is especially useful on a network where multiple multicast sources share the same multicast address.

Working Principle

Based on MLDv1, MLDv2 provides an extra function, that is, source filtering multicast. In MLDv1, a host determines to join a group only based on the group address and receives multicast streams sent to the group address from any source. However, an MLDv2 host advertises the multicast group that the host wants to join and the address of the multicast source that it wants to receive. In MLDv1,

source address filtering can be implemented to some extent, but filtering is implemented by enabling SSM-MAP and configuring SSM-MAP static groups on multicast flow receivers.

Related Configuration

❖ Enabling MLD SSM-MAP

By default, SSM-MAP is disabled.

Run the **ipv6 mld ssm-map enable** command to enable or disable the SSM-MAP function.

This function must be enabled when SSM-MAP is used.

❖ Configuring MLD SSM-MAP STATIC

By default, no SSM-MAP static link table is configured.

Run the **ipv6 mld ssm-map static access-list-num A.B.C.D** command to enable or disable the SSM-MAP static link table.

4.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of MLD	(Mandatory) It is used to configure the multicast service.	
	ipv6 multicast-routing	Enables the IPv6 multicast routing function.
	ipv6 pim sparse-mode	Enables the PIM-SM function.
Configuring MLD Router Parameters	ipv6 mld version { 1 2 }	Configures the MLD version.
	ipv6 mld last-member-query-interval interval	Configures the interval for querying the last member.
	ipv6 mld last-member-query-count count	Configures the number of times for querying the last member.
	ipv6 mld query-interval seconds	Configures the interval for querying a common member.
	ipv6 mld query-max-response-time seconds	Configures the maximum response interval.
Querier Selection Process or Timeout Mechanism	ipv6 mld querier-timeout seconds	Configures the keepalive interval of the querier.
Filtering MLD Groups	ipv6 mld access-group access-list	Filters MLD group members.
MLD Proxy	ipv6 mld proxy-service	Configures the MLD PROXY-SERVICE.
	ipv6 mld mroute-proxy interface-type interface-number	Configures the MLD MROUTE-PROXY.
Supporting SSM-MAP	ipv6 mld ssm-map enable	Enables the SSM-MAP function.
	ipv6 mld ssm-map static access-list source-address	Configures the SSM-MAP static link table.

4.4.1 Configuring Basic Functions of MLD

Configuration Effect

- Enable the multicast routing function and collect group information on the local network.

Notes

- The PIM SM function must be enabled on an interface.

Configuration Steps

- ❖ Enabling the IPv6 Multicast Routing Function
 - Mandatory.
 - The IPv6 multicast routing function should be enabled on all routers on the local network unless otherwise specified.
- ❖ Enabling the PIM SM Function
 - Mandatory.
 - The PIM SM function should be directly enabled on an interface on the local network unless otherwise specified.

Verification

Run the **show ipv6 mld interface *interface-type* *interface-number*** command to check whether MLD is enabled on the interface.

Related Commands

- ❖ Enabling the IPv6 Multicast Routing Function

Command	ipv6 multicast-routing
Parameter	N/A
Description	
Command Mode	Global configuration mode
Usage Guide	-

- ❖ Enabling the PIM SM Function

Command	ipv6 pim { sparse-mode }
Parameter	-
Description	
Command Mode	Interface configuration mode
Usage Guide	PIM interfaces must be layer-3 interfaces, including: routing, L3AP, SVI, and loopback interfaces. IPv6 unicast routes should be accessible to all PIM interfaces.

Configuration Example

❖ Enabling MLD on the Local Network

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure an IPv6 unicast routing protocol (such as OSPF) on a router and ensure that unicast routes are accessible to the loopback interface. (Omitted) ➤ Enable the IPv6 multicast routing function on all routers. ➤ Enable the PIM SM function on device interconnection interfaces and interfaces for connecting user hosts and multicast sources.
	<pre>VSU(config)#ipv6 multicast routing VSU(config)#int gi 0/1 VSU(config if GigabitEthernet 0/1)# ipv6 address 2001::1/64 VSU(config if GigabitEthernet 0/1)#ipv6 pim sparse mode</pre>
Verification	<p>Run the show ipv6 mld interface <i>interface-type</i> <i>interface-number</i> command to check whether MLD is enabled on the interface.</p>
	<pre>VSU#show ipv6 mld interface gigabitEthernet 0/1 Interface GigabitEthernet 0/1 (Index 1) MLD Active, Querier, Version 2 (default) Internet address is fe80::2d0:f8ff:fe22:33b1 MLD interface limit is 1024 MLD interface has 0 group record states MLD interface has 0 join group records MLD interface has 0 static group records MLD activity: 0 joins, 0 leaves MLD query interval is 125 seconds MLD querier timeout is 255 seconds MLD max query response time is 10 seconds Last member query response interval is 10 (1/10s) Last member query count is 2 Group Membership interval is 260 Robustness Variable is 2</pre>

Common Errors

- Multicast routing is disabled on routers on the network.
- No multicast interface is available on the network.

4.4.2 Configuring MLD Router Parameters**Configuration Effect**

- Modify MLD router parameters to change the message type or sending mode.

Notes

- The basic functions of MLD must be configured.

Configuration Steps

- ❖ Configuring MLD Version

Optional.

This parameter can be configured on all router interfaces directly connected to the local network unless otherwise specified.

- ❖ Configuring the Interval for Querying the Last Member

Optional.

This parameter can be configured on all router interfaces directly connected to the local network unless otherwise specified.

- ❖ Configuring the Number of Times for Querying the Last Member

Optional.

This parameter can be configured on all router interfaces directly connected to the local network unless otherwise specified.

- ❖ Configuring the Interval for Querying a Common Member

Optional.

This parameter can be configured on all router interfaces directly connected to the local network unless otherwise specified.

- ❖ Configuring the Maximum Response Interval

Optional.

This parameter can be configured on all router interfaces directly connected to the local network unless otherwise specified.

Verification

Run the **show ipv6 mld interface** *interface-type interface-number* command to view the configuration information.

Related Commands

- ❖ Configuring the MLD Version

Command	ipv6 mld version { 1 2 }
Parameter	1: Indicates version 1.
Description	2: Indicates version 2.

Command Mode	Interface configuration mode
Usage Guide	After this command is executed, MLD will automatically restart.

❖ Configuring the Interval for Querying the Last Member

Command	ipv6 mld last-member-query-interval <i>interval</i>
Parameter Description	<i>Interval</i> : Specifies the interval for sending Query messages of a specified group. The unit is 0.1s, the value ranges from 1 to 255, and the default value is 10 (1s).
Command Mode	Interface configuration mode
Usage Guide	After receiving the Done message, the interface will continuously send Query messages of a specified group and wait for responses from the host. After timeout, it is considered that the no group member exists in the directly-connected network segment and the interface is deleted from the MLD group member record. The timeout interval is calculated as follows: Timeout interval = last-member-query-interval x last-member-query-count + query-max-response-time/2.

❖ Configuring the Number of Times for Querying the Last Member

Command	ipv6 mld last-member-query-count <i>count</i>
Parameter Description	<i>count</i> : Specifies the number of times for sending Query messages of a specified group. The value ranges from 2 to 7. The default value is 2.
Command Mode	Interface configuration mode
Usage Guide	After receiving the Done message, the interface will continuously send Query messages of a specified group and wait for responses from the host. After timeout, it is considered that the no group member exists in the directly-connected network segment and the interface is deleted from the MLD group member record. The timeout interval is calculated as follows: Timeout interval = last-member-query-interval x last-member-query-count + query-max-response-time/2

❖ Configuring the Interval for Querying a Common Member

Command	ipv6 mld query-interval <i>seconds</i>
Parameter Description	<i>seconds</i> : Specifies the interval for querying a common member. The unit is s, the value ranges from 1 to 18000, and the default value is 125.
Command Mode	Interface configuration mode
Usage Guide	-

❖ Configuring the Maximum Response Interval

Command	ipv6 mld query-max-response-time <i>seconds</i>
Parameter Description	<i>seconds</i> : Specifies the maximum response time. The unit is s, the value ranges from 1 to 25, and the default value is 10.

Command Mode	Interface configuration mode
Usage Guide	After sending Query messages, the interface waits for responses. After timeout, it is considered that no group member exists in the directly-connected network segment and group information is deleted.

Configuration Example

❖ Configuring Basic Router Parameters

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of MLD. (Omitted) ➤ Configure MLD version 2. ➤ Configure the interval for querying the last member as 15 (1.5s). ➤ Configure the number of times for querying the last member as 3. ➤ Configure the interval for querying the common member as 130s. ➤ Configure the maximum response time as 15s.
	<pre>VSU(config if GigabitEthernet 0/1)#ipv6 mld version 2 VSU(config if GigabitEthernet 0/1)#ipv6 mld last member query count 3 VSU(config if GigabitEthernet 0/1)#ipv6 mld last member query interval 15 VSU(config if GigabitEthernet 0/1)#ipv6 mld query interval 130 VSU(config if GigabitEthernet 0/1)#ipv6 mld query max response time 15</pre>
Verification	Run the show ipv6 mld interface <i>interface-type interface-number</i> command to check whether MLD is enabled on the interface.
	<pre>VSU(config if GigabitEthernet 0/1)# show ipv6 mld interface gi 0/1 Interface GigabitEthernet 0/1 (Index 1) MLD Enabled, Active, Querier, Version 2 (default) Internet address is fe80::2d0:f8ff:fe22:33b1 MLD interface limit is 1024 MLD interface has 0 group record states MLD interface has 0 join group records MLD interface has 0 static group records MLD activity: 0 joins, 0 leaves MLD query interval is 130 seconds MLD querier timeout is 267 seconds MLD max query response time is 15 seconds Last member query response interval is 15 (1/10s)</pre>

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of MLD. (Omitted) ➤ Configure MLD version 2. ➤ Configure the interval for querying the last member as 15 (1.5s). ➤ Configure the number of times for querying the last member as 3. ➤ Configure the interval for querying the common member as 130s. ➤ Configure the maximum response time as 15s.
	<pre>VSU(config if GigabitEthernet 0/1)#ipv6 mld version 2 VSU(config if GigabitEthernet 0/1)#ipv6 mld last member query count 3 VSU(config if GigabitEthernet 0/1)#ipv6 mld last member query interval 15 VSU(config if GigabitEthernet 0/1)#ipv6 mld query interval 130 VSU(config if GigabitEthernet 0/1)#ipv6 mld query max response time 15</pre>
	<pre>Last member query count is 3 Group Membership interval is 275 Robustness Variable is 2</pre>

Common Errors

- Basic functions of MLD are not enabled.

4. 4. 3 Querier Selection Process or Timeout Mechanism

Configuration Effect

- Select the unique querier on the local network.

Notes

- The basic functions of MLD must be configured.

Configuration Steps

- This function must be configured if the querier keepalive interval needs to be configured.
- This function can be configured on all MLD-enabled interfaces on the local network.

Verification

Run the **show ipv6 mld interface *interface-type interface-number*** command to view the configuration information of the interface.

Related Commands

- ❖ Configuring the Keepalive Interval of Other Queriers

Command	ipv6 mld querier-timeout <i>seconds</i>
Parameter Description	<i>seconds</i> : Specifies the keepalive interval for other queriers. The unit is s, the value ranges from 60 to 300, and the default value is 255.
Command Mode	Interface configuration mode
Usage Guide	After sending Query messages, the interface waits for Query messages from other devices. After timeout, it is considered that it is the unique querier in the directly-connected network segment.

Configuration Example

- ❖ Configuring the Keepalive Interval of Other Queriers

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure the basic functions of MLD. (Omitted) ➤ Configure the keepalive interval of a querier as 280s.
	<pre>VSU(config-if GigabitEthernet 0/1)#ipv6 mld querier timeout 280</pre>
Verification	Run the show ipv6 mld interface <i>interface-type interface-number</i> command to check whether MLD is enabled on the interface.
	<pre>VSU#show ipv6 mld interface gigabitEthernet 0/1 Interface GigabitEthernet 0/1 (Index 1) MLD Enabled, Active, Querier, Version 2 (default) Internet address is fe80::2d0:f8ff:fe22:33b1 MLD interface limit is 1024 MLD interface has 0 group record states MLD interface has 0 join group records MLD interface has 0 static group records MLD activity: 0 joins, 0 leaves MLD query interval is 130 seconds MLD querier timeout is 280 seconds</pre>

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure the basic functions of MLD. (Omitted) ➤ Configure the keepalive interval of a querier as 280s.
	<pre>VSU(config if GigabitEthernet 0/1)#ipv6 mld querier timeout 280</pre>
	<pre>MLD max query response time is 15 seconds Last member query response interval is 15 (1/10s) Last member query count is 3 Group Membership interval is 275 Robustness Variable is 2</pre>

Common Errors

- The basic functions of MLD are not enabled.

4. 4. 4 Filtering MLD Groups

Configuration Effect

- A router filters MLD group information.

Notes

- The basic functions of MLD must be configured.

Configuration Steps

- ❖ Configuring Access Control for Multicast Groups

Optional.

This function can be configured on all router interfaces directly connected to the local network unless otherwise specified.

- ❖ Configuring the Maximum Number of MLD Group Members

Optional.

This function can be configured on all router interfaces directly connected to the local network unless otherwise specified.

Verification

- ❖ Filtering MLD Groups

Configure the interface to allow for only groups in link table 1. The access address of link table 1 is (FF66::100/64).

Configure the interface to add a group FF66::05.

Configure the interface to add a group FF65::05.

Check group information on the interface.

❖ Configuring the Maximum Number of MLD Group Members

Configure the number of group members as 5 on the interface.

Configure the interface to add a group (FF66::05~FF65::0B).

Check group information on the interface.

Related Commands

❖ Configuring Access Control for Multicast Groups

Command	ipv6 mld access-group <i>access-list</i>
Parameter Description	<i>access-list</i> : Specifies the group address range by using IP standard ACLs or IP extended ACLs. The value ranges from 1 to 199, 1300 to 2699, and WORD.
Command Mode	Interface configuration mode
Usage Guide	After running this command on the interface, you can control the groups that hosts in the directly-connected network segment can join. Use ACLs to limit the group address range. Report messages denied by the ACLs will be discarded. When MLDv2 is enabled, this command supports extended ACLs to precisely filter source record information in MLDv2 messages. When the received MLD Report message is (S1,S2,S3...Sn,G), this command will match (0,G) using the corresponding ACLs. Therefore, to normally use this command, you must explicitly configure a (0, G) in the extended ACLs to filter (S1,S2,S3...Sn,G).

❖ Configuring the Maximum Number of MLD Group Members

Command	ipv6 mld limit <i>number</i> [except <i>access-list</i>]
Parameter Description	<i>number</i> : Specifies the maximum number of MLD group members. The value range depends on the specific device. The interface default value is 1024 and the global one is 65536. except <i>access-list</i> : Groups in the access list are not counted. The access list is an IP standard ACL. The value ranges from 1 to 99, 1300 to 1999, and WORD.
Command Mode	Interface configuration mode
Usage Guide	Global configuration mode: Limits the number of MLD group members on the whole device. Interface configuration mode: Limits the number of MLD group members of the interface. If the number of group members exceeds the interface limit or global limit, subsequent Report messages will be ignored. If an except list is configured, Report messages in a specified range can be normally processed. Therefore, the group members are not counted. Interface and global limits can be configured separately. If the global limit is smaller than the interface limit, use the global limit.

Configuration Example

❖ Configuring Group Filtering

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure the basic functions of MLD. (Omitted) ➤ Configure the access address of link table 1 as (FF66::100/64). ➤ Configure the group to join as FF66::05. ➤ Configure the group to join as FF65::05.
	<pre>VSU(config)#ipv6 access list acl VSU(config ipv6 acl)#permit ipv6 ::/64 ff66::100/64 VSU(config ipv6 acl)#permit ipv6 2222::3333/64 ff66::100/64 VSU(config ipv6 acl)#exit VSU(config)# VSU(config)#int gi 0/1 VSU(config if GigabitEthernet 0/1)#ipv6 mld access group acl VSU(config if GigabitEthernet 0/1)#ipv6 mld join group ff66::5 VSU(config if GigabitEthernet 0/1)#ipv6 mld join group ff65::5</pre>
Verification	<p>Run the show ipv6 mld groups [interface-type interface-number] [group-address] [detail] command to view the group information on the interface.</p>
	<pre>VSU#show ipv6 mld groups MLD Connected Group Membership Group Address Interface Uptime Expires Last Reporter ff66::5 GigabitEthernet 0/1 00:05:07 00:03:46 fe80::2d0:f8ff:fe22:33b1</pre>

❖ Configuring the Maximum Number of MLD Group Members

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure the basic functions of MLD. (Omitted) ➤ Configure the maximum number of group members on the interface as 5. ➤ Add group information (FF66::5~FF66::0B). ➤ View the group information.
	<pre>VSU(config if GigabitEthernet 0/1)#ipv6 mld limit 5 VSU(config if GigabitEthernet 0/1)#ipv6 mld join group ff66::5 VSU(config if GigabitEthernet 0/1)#ipv6 mld join group ff66::6 VSU(config if GigabitEthernet 0/1)#ipv6 mld join group ff66::7 VSU(config if GigabitEthernet 0/1)#ipv6 mld join group ff66::8 VSU(config if GigabitEthernet 0/1)#ipv6 mld join group ff66::9 VSU(config if GigabitEthernet 0/1)#ipv6 mld join group ff66::A VSU(config if GigabitEthernet 0/1)#ipv6 mld join group ff66::B</pre>

Verification	Run the show ipv6 mld groups [<i>interface-type interface-number</i>] [<i>group-address</i>] [detail] command to view group information on the interface.		
	<pre> MLD Connected Group Membership Group Address Interface Uptime Expires Last Reporter ff66::5 GigabitEthernet 0/1 00:00:36 00:04:00 fe80::2d0:f8ff:fe22:33b1 ff66::6 GigabitEthernet 0/1 00:00:34 00:04:01 fe80::2d0:f8ff:fe22:33b1 ff66::7 GigabitEthernet 0/1 00:00:22 00:04:13 fe80::2d0:f8ff:fe22:33b1 ff66::8 GigabitEthernet 0/1 00:00:18 00:04:19 fe80::2d0:f8ff:fe22:33b1 ff66::9 GigabitEthernet 0/1 00:00:14 00:04:21 fe80::2d0:f8ff:fe22:33b1 </pre>		

Common Errors

- The basic functions of MLD are not enabled.

4.4.5 MLD Proxy

Configuration Effect

- Configure the router proxy function and collect local member information.

Notes

- The basic functions of MLD must be configured.

Configuration Steps

- ❖ Configuring MLD PROXY-SERVICE

Optional.

This function can be configured on the interface of routers directly connected to the upstream devices unless otherwise specified.

- ❖ Configuring MLD MROUTE-PROXY

Optional

This function can be configured on the interface of hosts directly connected to the downstream devices unless otherwise specified.

Verification

- Configure the interface that directly connects interface 7 and upstream router as the multicast proxy service.
- Configure the interface that directly connects interface 1 and downstream host as the multicast proxy.
- Configure groups FF66::05 and FF66::06 to be added to interface 1.
- Check information of the current group.

Related Commands

❖ Configuring MLD PROXY-SERVICE

Command	ipv6 mld proxy-service
Parameter Description	-
Command Mode	Interface configuration mode
Usage Guide	<p>Run the ipv6 mld proxy-service command to configure the upstream interface as the proxy-service interface.</p> <p>Run the ipv6 mld mroute-proxy command to configure the downstream interface as the mroute-proxy interface.</p> <p>Configure the proxy-service interface to forward MLD Query messages to the mroute-proxy interface.</p> <p>Configure the mroute-proxy interface to forward MLD Reports messages to the proxy-service interface.</p> <p>A maximum of 32 proxy-service interfaces can be configured on a device. After receiving MLD Query messages, the proxy-service interface sends a response based on the MLD group member records.</p> <p>If you run switchport command on the proxy-service interface, the ipv6 mld mroute-proxy command configured on the mroute-proxy interface will be automatically deleted.</p>

❖ Configuring MLD MROUTE-PROXY

Command	ipv6 mld mroute-proxy <i>interface-type interface-number</i>
Parameter Description	-
Command Mode	Interface configuration mode
Usage Guide	<p>Run the ipv6 mld proxy-service command to configure the upstream interface as the proxy-service interface.</p> <p>Run the ipv6 mld mroute-proxy command to configure the downstream interface as the mroute-proxy interface.</p> <p>Configure the proxy-service interface to forward MLD Query messages to the mroute-proxy interface.</p> <p>Configure the mroute-proxy interface to forward MLD Reports messages to the proxy-service interface.</p>

Configuration Example

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure MLD basic functions. (Omitted) ➤ Configure interface 7 as the proxy server. ➤ Configure interface 1 as the multicast proxy. ➤ Configure groups FF66::05 and FF66::06 to be added to interface 1.
	<pre>VSU(config if GigabitEthernet 0/7)#ipv6 mld proxy service VSU(config if GigabitEthernet 0/7)#exit VSU(config)#int gi 0/1 VSU(config if GigabitEthernet 0/1)#ipv6 mld mroute proxy gigabitEthernet 0/7 VSU(config if GigabitEthernet 0/1)#ipv6 mld join group ff66::05 VSU(config if GigabitEthernet 0/1)#ipv6 mld join group ff66::06</pre>
Verification	<p>Run the show ipv6 mld groups [interface-type interface-number] [group-address] [detail] command to view the group information on the interface.</p>
	<pre>VSU(config if GigabitEthernet 0/1)#show ipv6 mld groups MLD Connected Group Membership Group Address Interface Uptime Expires Last Reporter ff66::5 GigabitEthernet 0/1 00:00:11 00:04:31 fe80::2d0:f8ff:fe22:33b1 ff66::6 GigabitEthernet 0/1 00:00:11 00:04:33 fe80::2d0:f8ff:fe22:33b1 MLD Proxy server Connected Group Membership Group Address Interface Uptime ff66::5 GigabitEthernet 0/7 00:00:11 ff66::6 GigabitEthernet 0/7 00:00:11</pre>

Common Errors

- The basic functions of MLD are not enabled.

4. 4. 6 Supporting SSM-MAP

Configuration Effect

- MLDv2 supports source filtering while MLDv1 does not. However, MLDv1 provides the SSM-MAP function to implement source filtering.

Notes

- **The basic functions of MLD must be configured.**

Configuration Steps

❖ Enabling SSM-MAP

This function must be configured if SSM-MAP.

This function must be enabled on a router where SSM-MAP is enabled.

❖ Configuring an SSM-MAP Static Link Table

Optional.

This function must be enabled on a router where SSM-MAP is enabled.

Verification

Run the **show ipv6 mld ssm-mapping** [*group-address*] command to display SSM-MAP information.

Related Commands

❖ Enabling SSM-MAP

Command	ipv6 mld ssm-map enable
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	Run the ipv6 mld ssm-map enable command to enable the SSM-MAP function. Run the ipv6 mld ssm-map static command to configure static mapping table items. The interface runs MLDv2. When receiving Report messages from MLDv1, the interface adds the static mapping source address.

❖ Configuring an SSM-MAP Static Link Table

Command	ipv6 mld ssm-map static access-list source-address
Parameter Description	access-list: Specifies the group address range configured by the ACL. source-address: Source address
Command Mode	Global configuration mode
Usage Guide	Run the ipv6 mld ssm-map enable command to enable the SSM-MAP function. Run the ipv6 mld ssm-map static command to configure static mapping table items. The interface runs MLDv2. When receiving Report messages from MLDv1, the interface adds the static mapping source address.

Configuration Example

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure the basic functions of MLD. (Omitted) ➤ Enable SSM-MAP. ➤ Configure SSM-MAP static link table 3.
	VSU(config)#ipv6 mld ssm map enable

	<pre>VSU(config)#ipv6 mld ssm map static 3 1500::5</pre>
Verification	Run the show ipv6 mld ssm-mapping [group-address] command to view SSM mapping information.
	<pre>VSU(config)#show ipv6 mld ssm mapping SSM Mapping : Enabled Database : Static mappings configured</pre>

Common Errors

- The basic functions of MLD are not enabled.

4.5 Monitoring

Clearing

Description	Command
Clears dynamic group member records in the MLD cache.	clear ipv6 mld group [group-address] [interface-type interface-number]
Clears all MLD statistics and group member records on the interface.	clear ipv6 mld interface interface-type interface-number

Displaying

Description	Command
Displays groups directly connected to the device and group information learned from MLD.	show ipv6 mld groups [group-address interface-type interface-number] [detail]
Displays configurations of the interface.	show ipv6 mld interface [interface-type interface-number]
Displays SSM-MAP information.	show ipv6 mld ssm-mapping [group-address]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Displays the MLD debugging switch status.	show debugging
Debugs all MLD information.	debug ipv6 mld all
Debugs MLD packet resolution.	debug ipv6 mld decode
Debugs MLD packet encoding.	debug ipv6 mld encode
Debugs MLD event information.	debug ipv6 mld events
Debugs MLD Finite State Machine (FSM).	debug ipv6 mld fsm

Debugs MLD state machine information.	debug ipv6 mld tib
Debugs MLD warning.	debug ipv6 mld warning

5. CONFIGURING PIM-DM

5.1 Overview

Protocol Independent Multicast (PIM) is an intra-domain multicast routing protocol.

A multicast source sends a packet to a group address. The packet is forwarded by network devices hop by hop and finally reaches the group members. On layer-3 network devices, PIM is used to create and maintain multicast routing entries, so as to support multicast forwarding.

PIM works in two modes: Protocol Independent Multicast - Sparse Mode (PIM-SM) and Protocol Independent Multicast - Dense Mode (PIM-DM).

- PIM-SM is applicable to large-scale networks where group members are sparsely distributed in a wide scope.
- PIM-DM is applicable to small networks where group members are densely distributed.

Protocols and Standards

- RFC3973: Protocol Independent Multicast - Dense Mode (PIM-DM)
- RFC2715: Interoperability Rules for Multicast Routing Protocols

5.2 Applications

Application	Description
Providing the Multicast Service in the Same Network	The multicast service is provided in the same network.

5.2.1 Providing the Multicast Service in the Same Network

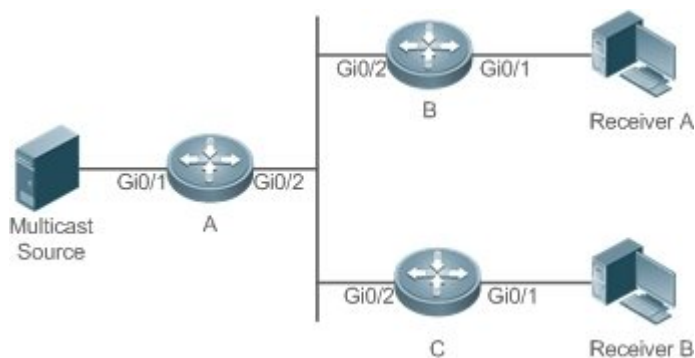
Scenario

The multicast service is provided in the same network.

The following figure is taken as an example:

- A multicast source sends a multicast packet, and Receiver A and Receiver B in the same network receive the multicast packet.

Figure 5-1



Remark	A, B, and C are Layer-3 routers.
s	The multicast source is connected to the Gi0/1 interface of A, Receiver A is connected to the Gi0/1 interface of B, and Receiver B is connected to Gi0/1 of C.

Deployment

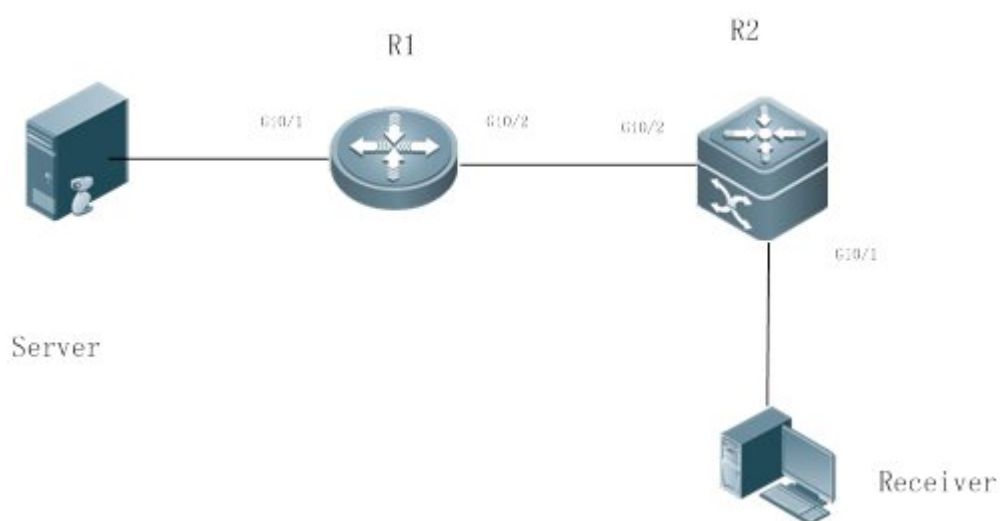
- Run the Open Shortest Path First (OSPF) protocol in the same network to implement unicast routing.
- Run the PIM-DM protocol in the same network to implement multicast routing.
- Run the Internet Group Management Protocol (IGMP) in a user host network segment to implement group member management.

1.1.1 PIM-DM Application in a Hot Backup Environment

Scenario

In a hot backup environment, run PIM-DM. A device performs hot backup switching to ensure that traffic is not interrupted.

Figure 5-2



Remarks	R1 is connected to the video server, R2 is directly connected to the receiver, and R2 runs in hot backup mode. A Layer-3 multicast protocol runs on R1 and R2.
----------------	---

Deployment

- Run OSPF on R1 and R2 to implement unicast routing.
- Run PIM-DM on R1 and R2 to implement multicast routing.
- Make R2 run in a hot backup environment.

Remarks	R2 may perform hot backup switching in the hot backup environment. In this case, the query interval of PIM Hello packets (the default value is 30 seconds) needs to be adjusted on R2 because the keepalive timer of the neighbor in PIM Hello packets of R1 may have expired (the default value is 3.5 times the query interval, that is, 105 seconds). The multicast function relies on the unicast function currently, and the multicast function starts convergence after the unicast function convergence is complete. For example, the default graceful restart (GR) convergence time of the unicast function is 120 seconds. It is recommended that the query interval of PIM Hello packets be set to 60 seconds. The keepalive time of the neighbor in PIM Hello packets is 210 seconds. In this scenario, the query interval of PIM Hello packets need to be set with a reference to the GR convergence time of the unicast function and the value of 3.5 times the query interval of PIM Hello packets must be larger than the GR convergence time of the unicast function. In a hot backup environment, it is recommended that the query interval of PIM Hello packets be larger than the default value (30 seconds). Otherwise, the keepalive timer of the neighbor in PIM Hello packets of the peer end times out during hot backup switching.
----------------	---

5.3 Features

Basic Concepts

❖ PIM Router and PIM Interface

Routers where the PIM protocol is enabled are called PIM Routers. Interfaces where the PIM protocol is enabled are called PIM interfaces.

Multicast packets are forwarded on PIM routers. The PIM interfaces where multicast packets are received are called Upstream Interfaces, and the PIM interfaces where multicast packets are sent are called Downstream Interfaces.

The network segments where upstream interfaces are located are called Upstream Network Segments. The network segments where downstream interfaces are located are called Downstream Network Segments.

❖ PIM Network and PIM Domain

PIM routers are connected through PIM interfaces and form a PIM network.

On some PIM interfaces, borders can be set to divide a large PIM network into multiple PIM domains. The borders are able to reject specified multicast packets or limit the transmission of PIM messages.

❖ Multicast Distribution Tree

Multicast packets are packets transmitted from one point to multiple points. The forwarding path is in a tree structure. This forwarding path is called the Multicast Distribution Tree (MDT).

❖ (*,G), (S,G)

- (*,G): Packets sent from any source to Group G, the corresponding routing entries, and the forwarding path called Rendezvous Point Tree (RPT).
- (S,G): Packets sent from Source S to Group G, the corresponding routing entries, and the forwarding path called Shortest Path Tree (SPT).

Overview

Feature	Description
PIM-DM Neighbor	Neighbor relationships are established between PIM routers to form a PIM network.
PIM-DM MDT	PIM-DM creates the MDT by using flooding, pruning, and grafting.
PIM-DM SRM	PIM-DM uses a State Refresh Message (SRM) to update the network state.
MIB	The Simple Network Management Protocol (SNMP) manager uses information in the Management Information Base (MIB) to directly manage the PIM-DM function.

5.3.1 PIM-DM Neighbor

Neighbor relationships are established between PIM routers to form a PIM network. Neighbor relationships must be established between PIM routers before PIM control messages can be exchanged or multicast packets can be forwarded.

Working Principle

A Hello message is sent from a PIM interface. For the IPv4 multicast packet with the Hello message encapsulated, the destination address is 224.0.0.13 (indicating all PIM routers in the same network segment), the source address is the IP address of the PIM interface, and the Time To Live (TTL) value is 1. For the IPv6 multicast packet with the Hello message encapsulated, the destination address is ff02::d.

Function of a Hello message: It is used to discover neighbors, coordinate protocol parameters, and maintain neighbor relationships.

❖ Discovering Neighbors

PIM routers in the same network segment receive multicast packets from the destination address 224.0.0.13 or ff02::d. In this way, the PIM routers obtain neighbor information and establish neighbor relationships.

When a PIM interface is enabled or detects a new neighbor, a Triggered-Hello-Delay message is used to generate a random time. Within the time, the interface sends Hello packets.

❖ Coordinating Protocol Parameters

A Hello message includes multiple protocol parameters, which are described as follows:

- DR_Priority: Router interfaces contend for the designated router (DR) based on their DR priorities. A higher priority means a higher chance of winning.
- Holdtime: Time in which a neighbor is held in the reachable state
- LAN_Delay: LAN delay for transmitting a Prune message in a shared network segment
- Override-Interval: Prune override time carried in a Hello message.

When a PIM router receives a Prune message from an upstream interface, it indicates that downstream interfaces exist in the shared network segment. If the PIM router still needs to receive multicast data, the PIM router must send a Prune Override message to the upstream interface within the Override-Interval.

$\text{LAN_Delay} + \text{Override-Interval} = \text{PPT}$ (Prune-Pending Timer). After a PIM router receives a Prune message from a downstream interface, the PIM router will not immediately perform pruning until PPT times out. Within the time of PPT, if the PIM router receives a Prune rejection message from the downstream interface, the PIM router cancels pruning.

❖ Maintaining Neighbor Relationships

A Hello message is sent periodically between PIM routers. If a Hello packet is not received from a PIM neighbor within Holdtime, the neighbor is considered unreachable and is deleted from the neighbor list. Any change of PIM neighbors will cause change of the multicast topology in the network. If an upstream or downstream neighbor in an MDT is unreachable, multicast routes converge again and the MDT is reshaped.

Related Configuration

❖ Enabling PIM-DM on an Interface

By default, PIM-DM is disabled on an interface.

Use the **ip pim dense-mode** command to enable or disable PIM-DM on an interface.

PIM-DM must be enabled on an interface to involve the interface in the PIM protocol.

❖ Setting the Interval of Hello Messages on an Interface

By default, a Hello message is sent at an interval of 30 seconds.

The **ip pim query-interval *interval-seconds*** command is used to adjust the interval of Hello messages. The value of the interval ranges from 1 to 65,535.

A Hello message is transmitted less frequently when the value of *interval-seconds* is larger.

5.3.2 PIM-DM MDT

PIM-DM creates the MDT by using flooding, pruning, and grafting.

Working Principle

When a multicast source sends multicast packets, the system may forward them to the outgoing interfaces of multicast neighbors and local members, depending on the results of the Reverse Path Forwarding (RPF) check. The packets not passing the RPF check are discarded. If an outgoing interface exists, the packets that have passed the RPF check are accepted for forwarding; if no outgoing interface exist, a prune packet is sent to upstream devices. After the upstream interface receives the prune packet, the upstream interface transmits the source interface of the prune packet as the Pruned state and sets the Prune Timer (PT). In this way, the MDT based on the multicast source is created.

When the system receives a Join message from a local member, if a downstream device in the Pruned state sends a Graft message to an upstream device, the upstream device returns a Graft Ack message and resume multicast forwarding to the interfaces of the downstream device after receiving the Graft message.

-
- In network deployment, when multiple PIM-DM neighbors are created through multiple links between devices and downstream devices have no or less need in receiving, the CPU usage may be high. In this scenario, PIM-SM is recommended to deploy the environment.
-

Related Configuration

- ❖ Configuring the Prune Override Interval on an Interface

By default, the prune override interval is 500 ms.

The **ip pim override-interval** *interval-milliseconds* command is used to modify the prune override interval.

5.3.3 PIM-DM SRM

PIM-DM uses an SRM to refresh the network state.

Working Principle

Devices connected to a multicast source periodically send SRMs to downstream devices to notify changes of the network topology. After receiving the SRMs, the adjacent devices receiving the SRMs add the local topology state information to the messages by modifying some fields in SRMs, and send the messages to downstream devices. When the messages reach leaf devices, the state information of the entire network is updated.

Related Configuration

- ❖ Disabling the Processing and Forwarding of SRMs

By default, the processing and forwarding of SRMs are enabled.

The **ip pim state-refresh disable** command is used to disable the processing and forwarding of SRMs.

- Disabling the SRM function may cause the converged PIM-DM MDT to re-converge, which leads to unnecessary bandwidth waste and multicast routing table flapping. Therefore, it is recommended not to disable SRM in general conditions.

❖ Setting the Interval of SRMs

By default, an SRM is sent at an interval of 60 seconds.

The **ip pim state-refresh origination-interval *interval-seconds*** command is used to adjust the interval of SRMs. The value of the interval ranges from 1 to 100.

SRMs are transmitted less frequently when the value of *interval-seconds* is larger.

- Only devices that are directly connected to a multicast source will periodically send a PIM SRM to downstream interfaces. For a device not directly connected to the multicast source, the interval of SRMs on its downstream interfaces is invalid.

5.3.4 MIB

Connected to other agents, the Simple Network Management Protocol (SNMP) manager uses information in the Management Information Base (MIB) to directly manage the PIM-DM function.

Working Principle

The MIB specifies variables (namely information that can be queried and set by the management process) maintained by network elements and directly manages the PIM-DM function.

Related Configuration

❖ Enabling PIM-DM MIB

By default, the PIM-DM MIB function is enabled.

The **ip pim mib dense-mode** command is used to enable the PIM-DM MIB function.

5.4 Configuration

Configuration	Description and Command
Configuring PIM-DM Basic Functions	(Mandatory) It is used to create the multicast service.
	ip multicast-routing Enables IPv4 multicast routing.
	ip pim dense-mode Enables PIM-DM.
Configuring PIM-DM Neighbors	(Optional) It is used to limit the (S,G) pairs of legitimate multicast packets in Any Source Multicast (ASM) model.

Configuration	Description and Command	
	ip pim query-interval <i>interval-seconds</i>	Sets the Interval of Hello messages on an interface.
	ip pim propagation-delay <i>interval-milliseconds</i>	Sets the prune propagation delay on an interface.
	ip pim override-interval <i>interval-milliseconds</i>	Sets the prune override interval on an Interface.
	ip pim neighbor-filter <i>access-list</i>	Configures neighbor filtering on an interface.
Configuring PIM-DM SRMs	ip pim state-refresh disable	Disables the processing and forwarding of SRMs.
	ip pim state-refresh origination-interval <i>interval-seconds</i>	Sets the Interval of SRMs on an interface.
Configuring PIM-DM MIB	ip pim mib dense-mode	Enables PIM-DM MIB.

5.4.1 Configuring PIM-DM Basic Functions

Configuration Effect

- Create a PIM-DM network and provide data sources and user terminals in the network with the IPv4 multicast service.

Notes

- PIM-DM needs to use the unicast routes existing in the network. Therefore, IPv4 unicast routing must be configured in the network.

Configuration Steps

- ❖ Enabling IPv4 Multicast Routing
 - Mandatory
 - IPv4 multicast routing should be enabled on each router unless otherwise specified.
- ❖ Enabling PIM-DM
 - Mandatory
 - PIM-DM should be enabled on the following interfaces unless otherwise specified: interconnected interfaces on routers and interfaces connecting multicast sources and user hosts.

Verification

Make multicast sources send multicast packets and make user hosts join the groups.

- Check whether the user hosts can successfully receive packets from each group.
- Check whether correct PIM-DM routing entries are created on routers.

Related Commands

❖ Enabling IPv4 Multicast Routing

Command	ip multicast-routing
Parameter	N/A
Description	
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Enabling PIM-DM

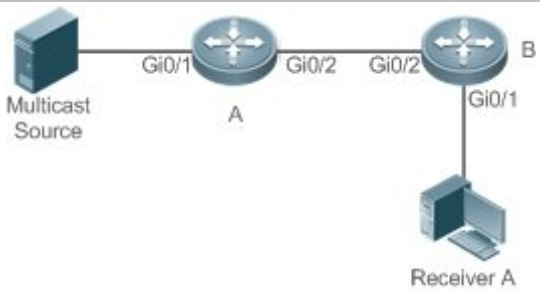
Command	ip pim dense-mode
Parameter	N/A
Description	
Command Mode	Interface configuration mode
Usage Guide	PIM interfaces must be at Layer-3, including: routing interfaces, aggregate ports(APs), switch virtual interfaces (SVIs), and loopback interfaces. For all PIM interfaces, IPv4 unicast routes should be reachable.

❖ Displaying the PIM-SM Routing Table

Command	show ip pim dense-mode mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]] [summary]
Parameter Description	<i>group-or-source-address</i> : Indicates a group address or source address. <i>group-or-source-address</i> : Indicates a group address or source address (The two addresses cannot be group addresses or source addresses at the same time). summary : Displays the routing table summary.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	Check whether sufficient routing entries are provided. Check the upstream and downstream interface lists and ensure that a correct SPT tree is created.

Configuration Example

❖ Enabling IPv4 Multicast Routing on the IPv4 Network

Scenario Figure 5-3	
Configuration Steps	<ul style="list-style-type: none"> ➤ Configure IPv4 unicast routing protocols (for example, OSPF) on all the routers. ➤ Enable the IPv4 multicast routing function on all the routers.

	<ul style="list-style-type: none"> ➤ Enable the PIM-DM function on all the interconnected interfaces of the routers, Source, and Receiver..
A	<pre>A# configure terminal A(config)# ip multicast routing A(config)# interface GigabitEthernet 0/1 A(config if)# ip pim dense mode A(config if)# exit A(config)# interface GigabitEthernet 0/2 A(config if)# ip pim dense mode A(config if)# exit</pre>
B	<pre>B# configure terminal B(config)# ip multicast routing B(config)# interface GigabitEthernet 0/1 B(config if)# ip pim dense mode B(config if)# exit B(config)# interface GigabitEthernet 0/2 B(config if)# ip pim dense mode B(config if)# exit</pre>
Verification	<p>Configure the multicast source (192.168.1.10) to send packets to G (229.1.1.1). Make Receiver A join G.</p> <ul style="list-style-type: none"> ➤ Check whether the multicast packets from Source G are received by Receiver A.. ➤ Check PIM-DM routing tables on Router A and Router B.
A	<pre>A# show ip pim dense mode mroute PIM DM Multicast Routing Table (192.168.1.10, 229.1.1.1) MRT lifetime expires in 182 seconds Source directly connected on GigabitEthernet 0/1 State Refresh Originator State: Originator SRT:57, SAT:147 Upstream IF: GigabitEthernet 0/1 Upstream State: Forwarding Assert State: NoInfo</pre>

	<pre> Downstream IF List: GigabitEthernet 0/2, in 'olist': Downstream State: NoInfo Assert State: NoInfo </pre>
B	<pre> B# show ip pim dense mode mroute PIM DM Multicast Routing Table (192.168.1.10, 229.1.1.1) MRT lifetime expires in 130 seconds RPF Neighbor: 192.168.2.1, Nexthop: 192.168.2.1, GigabitEthernet 0/2 Upstream IF: GigabitEthernet 0/2 Upstream State: Forwarding Assert State: Loser, AT:125 Downstream IF List: GigabitEthernet 0/1, in 'olist': Downstream State: NoInfo Assert State: NoInfo </pre>

Common Errors

- IPv4 unicast routing is incorrectly configured.
- IPv4 multicast routing is not enabled on a certain router.
- PIM-DM is not enabled on a certain interface.

5.4.2 Configuring PIM-DM Neighbors

Configuration Effect

- Coordinate protocol parameters and adjust parameters in the Hello packet.
- Enable neighbor filtering to improve network security.

Notes

- Basic functions of PIM-DM must be configured.

Configuration Steps

- Set parameters on PIM router interfaces unless otherwise specified.

Verification

- Set parameters in a Hello packet on an interface and run the **debug ip pim dense-mode encode** command to check parameters.
- Enable neighbor filtering and run the **show ip pim dense-mode decode** command to display neighbor filtering information.
- Run the **show running-config interface [interface-type interface-number]** command to display configurations on an interface.

Related Commands

❖ Setting the Interval of Hello Messages

Command	ip pim query-interval <i>interval-seconds</i>
Parameter Description	<i>interval-seconds</i> : The value ranges from 1 to 65,535 in the unit of seconds.
Command Mode	Interface configuration mode
Usage Guide	When the Hello interval is set, the holdtime value will be updated as its 3.5 times.
<ul style="list-style-type: none"> ➤ Every time when the interval of Hello messages is updated, the holdtime value is automatically updated as 3.5 times of the interval. If the result of the interval of Hello messages multiplied by 3.5 is greater than 65,535, the holdtime value is updated as 65,535. 	

❖ Setting the Prune Propagation Delay

Command	ip pim propagation-delay <i>interval-milliseconds</i>
Parameter Description	<i>interval-milliseconds</i> : The value ranges from 1 to 32,767 in the unit of milliseconds.
Command Mode	Interface configuration mode
Usage Guide	Set propagation-delay of an interface, that is, configure the prune propagation delay of an interface.

❖ Setting the Prune Override Interval

Command	ip pim override-interval <i>interval-milliseconds</i>
Parameter Description	<i>interval-milliseconds</i> : The value ranges from 1 to 32,767 in the unit of milliseconds.
Command Mode	Interface configuration mode
Usage Guide	Set override-interval of an interface, that is, configure the prune override time of an interface.


❖ Configuring PIM-DM Neighbor Filtering

Command	ip pim neighbor-filter <i>access-list</i>
Parameter Description	<i>access-list</i> : The supported ACL ranges from 1 to 99. Naming an ACL is also supported.

Command	Interface configuration mode
Mode	
Usage Guide	<p>Only addresses that meet ACL filtering conditions can be used as PIM neighbors of the current interface. Otherwise, the addresses filtered out cannot be neighbors.</p> <p>Peering refers to exchange of protocol packets between PIM neighbors. If peering with a PIM device is suspended, the neighbor relationship with it cannot be formed so that PIM protocol packets will not be received from the device.</p>


Configuration Example

❖ Configuring PIM-DM Neighbors on the IPv4 Network

Scenario Figure 5-4	
Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-DM (omitted). ➤ Set protocol parameters in a Hello packet on the Gi0/1 interface of device A.
A	<pre>A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if)# ip pim query interval 60 A(config-if)# ip pim propagation delay 800 A(config-if)# ip pim override interval 1000 A(config-if)# exit</pre>
Verification	<ul style="list-style-type: none"> ➤ Run the show running-config interface [interface-type interface-number] command to display configurations on an interface. ➤ Run the debug ip pim dense-mode encode command to debug parameters in a Hello packet.
A	<pre>A# (config)#show running config interface gigabitEthernet 0/1 Building configuration... Current configuration : 245 bytes ! interface GigabitEthernet 0/1 ip pim dense mode ip pim query interval 60</pre>

	<pre>ip pim propagation delay 800 ip pim override interval 1000</pre>
	<pre>A# debug ip pim dense mode encode *Dec 22 15:00:58: %7: [ENCODE] Enc Hello: Hello Hold Time 210 *Dec 22 15:00:58: %7: [ENCODE] Enc Hello: Hello Gen ID 1362200073 *Dec 22 15:00:58: %7: [ENCODE] Enc Hello: Hello PD=800 ms, OI=1000 ms *Dec 22 15:00:58: %7: [ENCODE] Enc Hello: Hello SR Interval 60 *Dec 22 15:00:58: %7: [ENCODE] Enc Msg Hdr: Hello Checksum=65396, MsgLen=34 Assert State: Loser, AT:125</pre>

❖ Configuring PIM-DM Neighbor Filtering on the IPv4 Network

Scenario Figure 5-5	
Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-DM (omitted). ➤ Configure an ACL on device A. ➤ Configure PIM neighbor filtering on the Gi0/1 interface of device A.
A	<pre>A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config if)# ip pim query interval 60 A(config if)# ip pim propagation delay 800 A(config if)# ip pim override interval 1000 A(config if)# exit</pre>
Verification	<ul style="list-style-type: none"> ➤ Run the show running-config interface [interface-type interface-number] command to display configurations on the interface. ➤ Run the debug ip pim dense-mode decode command to debug parameters in a Hello packet.
A	<pre>A#show running config interface gigabitEthernet 0/2 Building configuration... Current configuration : 187 bytes</pre>

<pre>! interface GigabitEthernet 0/1 ip pim dense mode ip pim neighbor filter pim dm</pre>
<pre>A# debug ip pim dense mode decode Dec 22 15:15:47: %7: [DECODE] Dec Msg: PIM Hello message, version 2 Dec 22 15:09:47: %7: [DECODE] Dec Msg: Neighbor 192.168.2.2/32 on GigabitEthernet 0/1 denied by access list pim dm</pre>

Common Errors

- IPv4 unicast routing is incorrectly configured.
- IPv4 multicast routing is not enabled on a certain router.
- PIM-DM is not enabled on a certain interface.

5.4.3 Configuring PIM-DM SRMs

Configuration Effect

- Enable or disable the PIM-DM SRM function.
- Adjust the interval of SRMs.

Notes

- Basic functions of PIM-DM must be configured.

Configuration Steps

- The interval of SRMs is only applicable only to the PIM router interfaces that are directly connected to the multicast source.

Verification

- Configure the PIM-DM SRMs and run the **show running-config** command to display the SRM status.
- Run the **show ip pim dense-mode track** command to display the SRM number.
- Run the **show running-config interface** [*interface-type interface-number*] command to display interface configurations.

Related Commands

- ❖ Disabling the Processing and Forwarding of SRMs

Command	ip pim state-refresh disable
Parameter	N/A
Description	

Command Mode	Global configuration mode
Usage Guide	When the processing and forwarding of SRMs are disabled, the State Refresh Capable option is not included in a Hello packet, and is not processed when the Hello packet is received. Disabling the SRM function may cause the converged PIM-DM MDT to re-converge, which leads to unnecessary bandwidth waste and multicast routing table flapping. Therefore, it is recommended not to disable this function in general conditions.

❖ Setting the Interval of SRMs

Command	<code>ip pim state-refresh origination-interval interval-seconds</code>
Parameter Description	<i>interval-seconds</i> : The value ranges from 1 to 100 in the unit of second.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

❖ Disabling the Processing and Forwarding of SRMs on an Interface on the IPv4 Network

Scenario Figure 5-6	
Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-DM (omitted). ➤ Disable processing and forwarding of a PIM-DM SRM on an Interface of device A.
A	<pre>A# configure terminal A(config)# ip pim state refresh disable</pre>
Verification	<ul style="list-style-type: none"> ➤ Run the show running-config command to check the configuration.
A	<pre>A# (config)# show running config ... ! ip pim state refresh disable !</pre>

	...
--	-----

❖ Setting the Interval of SRMs on the IPv4 Network

<p>Scenario Figure 5-7</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-DM (omitted). ➤ Set the interval of PIM-DM SRMs on the Gi0/1 interface of device A.
<p>A</p>	<pre>A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if)# ip pim state refresh origination interval 5 A(config-if)# exit</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ➤ Run the show running-config interface [interface-type interface-number] command to display interface configurations. ➤ Run the show ip pim dense-mode track command to display the SRM number.
<p>A</p>	<pre>A#show running config interface gigabitEthernet 0/1 Building configuration... Current configuration : 201 bytes ! interface GigabitEthernet 0/1 ip pim dense mode ip pim state refresh origination interval 5</pre>
	<pre>A #show ip pim dense mode track PIM packet counters Elapsed time since counters cleared: 00:18:54 received sent</pre>

Valid PIMDM packets:	38	102
Hello:	38	76
Join/Prune:	0	0
Graft:	0	0
Graft Ack:	0	0
Assert:	0	0
State Refresh:	0	26
PIM SM Register:	0	
PIM SM Register Stop:	0	
PIM SM BSM:	0	
PIM SM C RP ADV:	0	
Unknown Type:	0	
Errors:		
Malformed packets:	0	
Bad checksums:	0	
Unknown PIM version:	0	
Send errors:	0	

Common Errors

- IPv4 unicast routing is incorrectly configured.
- IPv4 multicast routing is not enabled on a certain router.
- PIM-DM is not enabled on a certain interface.

5.4.4 Configuring PIM-DM MIB

Configuration Effect

- Enable the MIB function for PIM-DM.

Verification

- Configure the MIB function of PIM-SM and run the **show running-config** command to check whether the function is configured.

Related Commands

- ❖ Enabling PIM-DM MIB

Command	ip pim mib dense-mode

Parameter	N/A
Description	
Command Mode	Global configuration mode
Usage Guide	N/A

5.5 Monitoring

Clearing

Description	Command
Resets the statistic start time and clears the counters of PIM-DM packets.	clear ip pim dense-mode track

Displaying

Description	Command
Displays the help information of the commands with IP PIM as the key word.	ip pim help
Displays help information about configuration examples.	pim-dm help
Displays PIM-DM information of an interface.	show ip pim dense-mode interface [<i>interface-type interface-number</i>] [detail]
Displays the PIM-DM neighbors.	show ip pim dense-mode neighbor [<i>interface-type interface-number</i>]
Displays the PIM-DM next-hop information .	show ip pim dense-mode nexthop
Displays the PIM-DM routing table.	show ip pim dense-mode mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]] [summary]
Displays the number of PIM-DM packets sent and received since the statistic start time.	show ip pim dense-mode track
Displays the PIM-DM running status.	view pim-dm

6. CONFIGURING PIM-SM

6.1 Overview

Protocol Independent Multicast (PIM) is an intra-domain multicast routing protocol.

A multicast source sends a packet to a group address. The packet is forwarded by network devices hop by hop and finally reaches the group members. On Layer-3 network devices, PIM is used to create and maintain multicast routing entries, so as to support multicast forwarding.

PIM works in two modes: Protocol Independent Multicast - Sparse Mode (PIM-SM) and Protocol Independent Multicast - Dense Mode (PIM-DM).

- PIM-SM is applicable to large-scale networks where group members are sparsely distributed in a wide scope.
- PIM-DM is applicable to small networks where group members are densely distributed.

Protocols and Standards

- RFC4601: Protocol Independent Multicast -Sparse Mode (PIM-SM)
- RFC5059: Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
- RFC3962: Protocol Independent Multicast - Dense Mode protocol
- RFC4607: Source-Specific Multicast for IP

6.2 Applications

Application	Description
Enabling ASM for PIM-SM	The receiver receives any multicast source.
Enabling SSM for PIM-SM	The receiver receives only a specific multicast source.

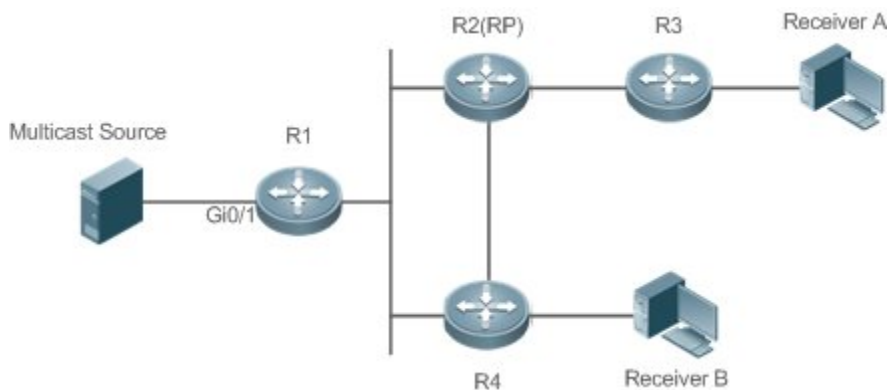
6.2.1 Enabling ASM for PIM-SM

Scenario

Provide multicast services within only one domain.

For example, in the following figure, the receiver receives any multicast source.

Figure 6-1



Remark	R 1 is connected directly to the multicast source.
s	R 2 serves as the rendezvous point (RP).
	R 3 is connected directly to Receiver A.
	R 4 is connected directly to Receiver B.

Deployment

- Run the Open Shortest Path First (OSPF) protocol to realize unicast routing.
- Run PIM-SM to realize multicast routing.
- Run the Internet Group Management Protocol (IGMP) in the network segment of the user host to manage group members.

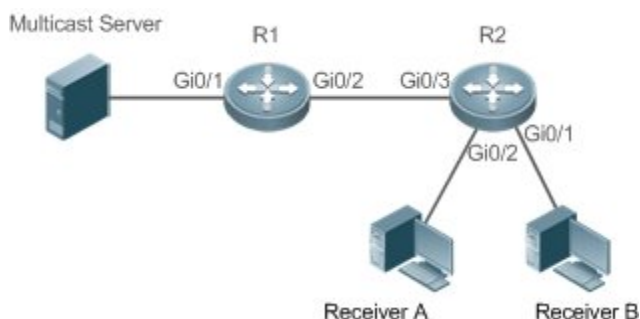
6. 2. 2 Enabling SSM for PIM-SM

Scenario

Provide multicast services within only one domain.

For example, in the following figure, the receiver receives a specific multicast source.

Figure 6-2



Remark	R 1 is connected directly to the multicast source.
s	R 2 serves as the RP.
	R 2 is connected directly to Receiver A.
	R 2 is connected directly to Receiver B.

Deployment

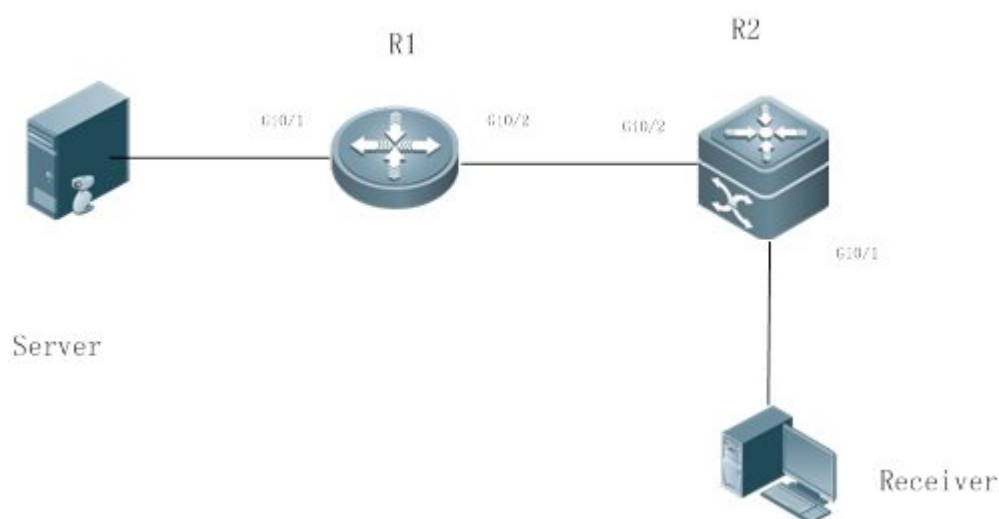
- Run the OSPF protocol to realize unicast routing.
- Run PIM-SM to realize multicast routing.
- Run the source-specific multicast (SSM) of PIM-SM within the domain.
- Run IGMPv3 in the network segment of the user host to manage group members.

1.1.2 PIM-SM Application in a Hot Backup Environment

Scenario

In a hot backup environment, run PIM-SM. A device performs hot backup switching to ensure that traffic is not interrupted.

Figure 6-3



Remarks	<p>R1 is connected to the video server, R2 is directly connected to the receiver, and R2 runs in hot backup mode.</p> <p>A Layer-3 multicast protocol runs on R1 and R2.</p>
----------------	--

Deployment

- Run OSPF on R1 and R2 to implement unicast routing.
- Run PIM-SM on R1 and R2 to implement multicast routing.
- Make R2 run in a hot backup environment.

Remarks	<p>R2 may perform hot backup switching in the hot backup environment. In this case, the query interval of PIM Hello packets (the default value is 30 seconds) needs to be adjusted on R2 because the keepalive timer of the neighbor in PIM Hello packets of R1 may have expired (the default value is 3.5 times the query interval, that is, 105 seconds). The multicast function relies on the unicast function currently, and the multicast function starts convergence after the unicast function convergence is complete. For example, the default graceful restart (GR) convergence time of the unicast function is 120 seconds. It is recommended that the query interval of PIM Hello packets be set to 60 seconds.</p>
----------------	---

The keepalive time of the neighbor in PIM Hello packets is 210 seconds. In this scenario, the query interval of PIM Hello packets need to be set with a reference to the GR convergence time of the unicast function and the value of 3.5 times the query interval of PIM Hello packets must be larger than the GR convergence time of the unicast function. In a hot backup environment, it is recommended that the query interval of PIM Hello packets be larger than the default value (30 seconds). Otherwise, the keepalive timer of the neighbor in PIM Hello packets of the peer end times out during hot backup switching.

6.3 Features

Basic Concepts

❖ PIM Router and PIM Interface

A router running PIM is called a PIM router. An interfaces running PIM is called a PIM interface.

Multicast packets are forwarded on PIM routers. The PIM interfaces where multicast packets are received are called upstream interfaces, and the PIM interfaces where multicast packets are sent are called downstream interfaces.

The network segments where upstream interfaces are located are called upstream network segments, and the network segments where downstream interfaces are located are called downstream network segments.

❖ PIM Network and PIM Domain

PIM routers are connected through PIM interfaces to form a PIM network.

On some PIM interfaces, borders can be set to divide a large PIM network into multiple PIM domains. The borders can reject the passage of specific multicast packets or limit the transmission of PIM packets.

❖ Multicast Distribution Tree, DR, and RP

Multicast packets are transmitted from one point to multiple points, forming a tree-shaped forwarding path. Such forwarding path is called the multicast distribution tree (MDT), which includes the following two types:

- RP Tree (RPT): It is rooted at an RP, and uses the designated router (DR) of the member groups connected to it as its leaves.
- Shortest path tree (SPT): It is rooted at a DR that is connected to the multicast source, and uses the RP or the DR of the member groups connected to it as its leaves.

Both the DR and RP are the functions of a PIM router.

- An RP collects the information of a multicast source or multicast member on the network.
- The DR connected to the multicast source advertises the multicast source information to the RP; the DR connected to multicast group members advertises the information of multicast group members to the RP.
- ❖ (*, G), (S, G)
 - (*, G): Indicates the packets sent from any source to a group (G), the corresponding route entries, and the RPT.
 - (S, G): Indicates the packets sent from the source (S) to a group (G), the corresponding routing entries, and the SPT.
- ❖ ASM, SSM

PIM-SM supports both any-source multicast (ASM) and SSM, and it is applicable to different multicast group address segments.

- ASM: In this model, a user is not allowed to select a multicast source. The user host joins a group, and receives the packets sent from all sources.
- SSM: In this model, a user can select a multicast source. The user host joins a group and specifies the source address. Then only the packets sent from this source address is received.

i Requirements for using an SSM model: Before selecting a multicast source, you need to learn the address of the multicast source using other network services.

Overview

Feature	Description
PIM-SM Neighbor	Establishes neighbor relationships between PIM routers to form a PIM network.
DR Election	In the network segment where group member hosts are located, PIM neighbors compete for the DR, and the one wins the election becomes the DR for connecting to the group members. In the network segment where the multicast source is located, PIM neighbors compete for the DR, and the one wins the election becomes the DR for connecting to the multicast source.
BSR Mechanism	On a PIM network, the BSR generates periodic candidate RPs and bootstrap packets of corresponding group addresses.
RP Mechanism	On a PIM network, through static RP configuration or dynamic RP election, the location of the RP can be learned by each PIM router.
Register Information of the Multicast Source	When the multicast source is detected on the network, the source DR sends a register packet to the RP, which obtains the source information and multicast packet.
Creating an RPT	When a group member is detected on the network, the DR connecting to the group members send packets toward the RP to form an RPT. If the multicast source already exists on the network, the packets arrived at the RP can be sent to the group members along the RPT.
Creating an SPT	When data packets arrive at the DR connecting to group members, the DR sends these packets toward the multicast source to form an SPT, and multicast packets are sent to group members along the SPT.

Feature	Description
ASM and SSM	A PIM router can provide multicast services of both ASM model and SSM model at the same time. SSM model applies to the groups whose addresses are within the range of the SSM addresses. For other groups, use ASM model.

6.3.1 PIM-SM Neighbor

Neighbor relationships are established between PIM routers to form a PIM network. Neighbor relationships must be established between PIM routers before PIM control packets can be exchanged or multicast packets can be forwarded.

Working Principle

A PIM interface sends a Hello packet. For the IPv4 multicast packet whose Hello packet is encapsulated, the destination address is 224.0.0.13 (indicating all PIM routers in the same network segment), the source address is the IP address of the PIM interface, and the Time To Live (TTL) value is 1. For the IPv6 multicast packet whose Hello packet is encapsulated, the destination address is ff02::d.

A Hello packet is used to discover neighbors, coordinate protocol parameters, and maintain neighbor relationships.

❖ Discovering Neighbors

PIM routers in the same network segment receive multicast packets from the destination address 224.0.0.13. In this way, the PIM routers obtain neighbor information and establish neighbor relationships.

When a PIM interface is enabled or detects a new neighbor, a triggered-hello-delay packet is used to generate a random time. Within the time, the interface sends Hello packets.

❖ Coordinating Protocol Parameters

A Hello packet includes multiple protocol parameters, which are described as follows:

- DR_Priority: indicates the priority of a router interface for competing for the DR. A higher priority means a higher chance of winning.
- Holdtime: Indicates the time in which a neighbor is held in the reachable state
- LAN_Delay: Indicates the LAN delay for transmitting a Prune packet in a shared network segment.
- Override-Interval: Indicates the prune override time carried in a Hello packet.

When a PIM router receives a Prune packet from an upstream interface, it indicates that downstream interfaces exist in the shared network segment. If the PIM router still needs to receive multicast data, the PIM router must send a Prune Override packet to the upstream interface within the override interval.

$LAN_Delay + Override\ Interval = PPT$ (Prune-Pending Timer). After a PIM router receives a Prune packet from a downstream interface, the PIM router will not immediately perform pruning until PPT

times out. Within the time of PPT, if the PIM router receives a Prune rejection packet from the downstream interface, the PIM router cancels pruning.

❖ Maintaining Neighbor Relationships

A Hello packet is sent periodically between PIM routers. If a Hello packet is not received from a PIM neighbor within Holdtime, the neighbor is considered unreachable and is deleted from the neighbor list. Any change of PIM neighbors will cause change of the multicast topology in the network. If an upstream or downstream neighbor in an MDT is unreachable, multicast routes converge again and the MDT is reshaped.

Related Configuration

❖ Enabling PIM-SM on an Interface

By default, PIM-SM is disabled on an interface.

Run **ip pim sparse-mode** to enable or disable PIM-SM on an interface.

PIM-SM must be enabled on an interface to involve the interface in the PIM protocol. If PIM-SM is not enabled for the interface of a DR, static RP, candidate RP (C-RP), or candidate BSR (C-BSR), corresponding roles of the PIM protocol cannot be run.

❖ Setting the Interval of Hello Packets on an Interface

By default, a Hello packet is sent every 30s.

Run **ip pim query-interval *interval-seconds*** to adjust the interval of Hello packets. The value ranges from 1 to 65, 535.

A Hello packet is transmitted less frequently when the value of *interval-seconds* is greater.

6.3.2 DR Election

In the network segment where group member hosts are located, PIM neighbors compete for the DR, and the one wins the election becomes the DR for connecting to the group members.

In the network segment where the multicast source is located, PIM neighbors compete for the DR, and the one wins the election becomes the DR for connecting to the multicast source.

The DR sends Join/Prune packets toward the MDT, or sends the multicast source data to the MDT.

Working Principle

When creating a PIM neighbor, you can send a Hello packet to obtain the IP address and DR priority of the neighbor to elect a DR.

Two parameters play a key role in winning the DR election: the DR priority of an interface and the IP address of the interface.

❖ DR Priority of an Interface

During the DR election, the RIM router with the highest DR priority will be elected as the DR.

❖ Interface IP Address

During the DR election, if the priority of interfaces is the same, then interface IP addresses will be compared. The interface with the maximum IP address will be elected as the DR.

Related Configuration

❖ Enabling PIM-SM on an Interface

By default, PIM-SM is disabled on an interface.

Run **ip pim sparse-mode** to enable or disable PIM-SM on an interface.

PIM-SM must be enabled on an interface to involve the interface in the PIM protocol. If PIM-SM is not enabled for the interface of a DR, static RP, C-RP, or C-BSR, corresponding protocols cannot be run.

❖ Adjusting the DR Priority of an Interface

By default, the DR priority is 1.

Run **ip pim dr-priority *priority-value*** to adjust the DR priority of the interface. The value ranges from 0 to 4,294,967,294.

The DR priority is used in the DR election in the network segment directly connected the interface. A greater value indicates a higher priority.

6.3.3 BSR Mechanism

On a PIM network, the BSR generates periodic candidate RPs and bootstrap packets of corresponding group addresses. These bootstrap packets are sent hop by hop in the domain. All the routers on the entire network will receive these bootstrap packets, and record these candidate RPs and their corresponding group addresses.

Working Principle

One or multiple candidate BSRs are configured in a PIM-SM domain. You need to apply a certain algorithm to select the BSR from these candidate BSRs.

Related Configuration

❖ Configuring Candidate BSRs

By default, candidate BSRs are not configured.

Run **ip pim bsr-candidate *interface-type interface-number* [*hash-mask-length* [*priority-value*]]** to configure or cancel the configuration of candidate BSRs.

Through bootstrap packet (BSM) learning and competition of candidate BSRs, a unique BSR is generated for the PIM-SM domain.

❖ Configuring BSR Borders

By default, BSR borders are not configured.

Run **ip pim bsr-border** to configure or cancel the configuration of BSR borders.

After this command is configured, BSMs received by the interface will be discarded and will not be forwarded by this interface, preventing BSM flooding.

❖ Filtering BSMs

By default, BSMs from the BSR are not filtered.

Run **ip pim accept-bsr list** { <1-99> | <1300-1999> | *WORD* } to configure whether to filter BSMs.

If this function is enabled, only legible BSMs are received by the interface; if this function is disabled, all the external BSMs will be received by the device running PIM-SM.

❖ Configuring Legible C-RP Addresses and the Multicast Groups They Serve for a Candidate BSR

By default, Candidate-RP-Advertisement (C-RP-Adv) packets are not filtered by a candidate BSR.

Run **ip pim accept-crp list** { <100-199> | <2000-2699> | *WORD* } to configure whether to filter C-RP-Adv packets.

If this function is enabled, C-RP addresses and corresponding multicast groups are filtered by a candidate BSR. If this function is disabled, all external C-RP-Adv packets are received by a candidate BSR.

❖ Allowing a C-BSR to Receive a C-RP-ADV Packet Whose Prefix-Count Is 0

By default, a candidate BSR cannot receive a C-RP-ADV packet whose prefix-count is 0.

Run **ip pim accept-crp-with-null-group** to configure whether to receive a C-RP-ADV packet whose prefix-count is 0.

If this function is enabled, a C-RP-ADV packet whose prefix-count is 0 can be received by a candidate BSR. If this function is disabled, a C-RP-ADV packet whose prefix-count is 0 cannot be received by a candidate BSR.

6.3.4 RP Mechanism

On a PIM network, through static RP configuration or dynamic RP election, the location of the RP can be learned by each PIM router. The RP as the root of the RPT, is the point where the RPT is rooted at and RPT data traffic is forwarded from.

Working Principle

All PIM routers in the same PIM domain must be mapped to the same RP as a specific multicast group address. On a PIM network, an RP can be configured as static or dynamic.

❖ Static RP

In static RP configuration, RP addresses are configured directly on PIM routers and these addresses are learnt by the entire PIM network.

❖ Dynamic RP

In a PIM-SM domain, there are candidate RPs that send unicast packets (including RP addresses and the multicast groups they serve) to the BSR, which generates periodic candidate RPs and bootstrap packets of corresponding group addresses. These bootstrap packets are sent hop by hop in the domain, and received and saved by PIM routers, which apply a hash function to map the group addresses to the candidate RP that can provide services. Then the RP corresponds to these multicast group addresses can be confirmed.

Related Configuration

❖ Configuring Static RP Addresses

By default, no RP address is configured.

Run **ip pim rp-address** *rp-address* [*access-list*] to configure a static RP address for a PIM router.

To use static RP addresses, the static RP address of all routers in the PIM-SM domain must be the same, so that the PIM SM multicast routing remains consistent.

❖ Configuring Candidate C-RP Addresses

By default, no C-RP address is configured.

Run **ip pim rp-candidate** *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *access-list*] to configure or cancel a PIM router as a candidate C-RP.

After a candidate RP is configured, it can send periodic C-RP-Adv packets to the BSR, and the information carried by these C-RP-Adv packets will be advertised to all PIM-SMs in the domain, ensuring the uniqueness of RP mapping.

❖ Ignoring the RP Priority in RP-Set

By default, C-RP of the highest priority is configured.

Run **ip pim ignore-rp-set-priority** to select or deselect the RP priority when selecting the corresponding RP of a multicast group.

If you want to select an RP from multiples RPs that serve the same multicast group address, you can run this command to ignore the RP priority. If this command is not configured, RP priority will be considered when two RPs are compared.

6.3.5 Register Information of the Multicast Source

When the multicast source is detected on the network, the source DR sends a register packet to the RP, which obtains the source information and multicast packet.

Working Principle

When a source DR receives a multicast packet from the host directly connected to it, the source DR encapsulates the multicast packet into the register packet, and sends the unicast packet to RP to form an (S, G) entry.

If the RP has an outgoing interface for the forwarding entry, it encapsulates the data packet and forwards the packet to the outgoing interface.

If the RP does not have the forwarding entry of the present group, it generates the (S, G) entry and enables the timer. If the timer times out, the RP sends a Register-Stop packet to the DR to delete the entry. The source DR sends an inspection packet before timeout after it receives the Register-Stop packet.

If no Register-Stop packet is received by the DR, the DR on the timeout data source will encapsulate the multicast data in the register packet and send the unicast packet to the RP.

If a Register-Stop packet is received by the DR, time-delay will be performed once again, and an inspection packet will be sent before time delay.

Related Configuration

❖ Detecting the Reachability of a Register Packet

By default, the reachability of an RP is not detected.

Run **ip pim register-rp-reachability** to configure or cancel the detection of the reachability of an RP.

You can enable this function if you want to detect whether an RP is reachable for a register packet sent from a DR. After this function is enabled, the DR will detect the reachability of a register packet before it is sent to an RP, namely, the DR will check whether a route to the RP exists in the unicast routing entry and static multicast routing entry. If the route does not exist, the register packet will not be sent.

❖ Configuring an RP to Filter the Addresses of Register Packets

By default, all register packets are received an RP.

Run **ip pim accept-register { list access-list [route-map map-name] / route-map map-name [list access-list] }** to configure an RP to filter or cancel the filtering of the source addresses of received register packets.

You can run this command if you want to filter the source addresses of received register packets. If this function is not enabled, all register packets will be received by the RP. If this function is disabled, only the register packets whose source addresses and multicast group addresses included in access control lists (ACLs) are processed; otherwise, the packets will be filtered.

❖ Limiting the Speed for Sending a Register Packet

By default, the speed for sending a register packet is not limited.

Run **ip pim register-rate-limit** *rate* to limit or cancel the limitation of the speed for sending a register packet.

If the **no** form of this command is configured, the speed is not limited. This command takes effect for only the register packet of each (S, G) packet, but not all the register packets in the entire system.

❖ Calculating the Checksum of the Entire Register Packet Length

By default, the checksum of a register packet is calculated as stipulated by the protocol.

Run **ip pim register-checksum-wholepkt** [**group-list** *access-list*] to configure the checksum of the register packet length.

You can enable this function if you want to include the length of encapsulated multicast packets into the checksum of the register packet length. If this function is disabled, the checksum of a register packet is calculated as stipulated by the protocol.

❖ Configuring an RP to Forward Multicast Data Packets to Downstream Interfaces After Decapsulating Register Packets

By default, register packets are not decapsulated and multicast packet are not forwarded to interfaces.

Run **ip pim register-decapsulate-forward** to forward or cancel the forwarding of data packets to downstream interfaces.

You can run this command if you want to decapsulate a register packet and forward the multicast packet. If this function is disabled, the multicast packet will not be forwarded.

❖ Configuring the Source IP Address of a Register Packet

By default, the source IP address of a register packet is the same as the interface address of the DR connected to the multicast source.

Run **ip pim register-source** { *local_address* | *Interface-type interface-number* } to configure the source IP address.

You can run this command is you want to configure the source IP address of the register packet sent by a DR. If this function is disabled or the **no** form of this command is used, the source address of the register packet will be the same as the interface address of the DR connected to the multicast

source. If you want to configure *local_address*, the configured address must be reachable for a unicast route. *Interface-type interface-number* can be a typical a loopback interface or an interface of other types. The interface address must have been advertised by a unicast route.

❖ Configuring the Suppression Time of a Register Packet

By default, the suppression time of a register packet is 60s.

Run **ip pim register-suppression seconds** to configure the suppression time.

If you run this command on a DR, you can change the suppression time of the register packets sent from the DR. If you run this command but does not run **ip pim rp-register-kat** on an RP, the keepalive period of the RP will be changed.

❖ Configuring the Inspection Time of a Null Register Packet

By default, the inspection time is 5s.

Run **ip pim probe-interval interval-seconds** to configure the inspection time.

In the time interval before the timeout of register packet suppression, the source DR can send a null register packet to an RP. This time interval is called the inspection time, which is 5s by default.

❖ Configuring the Time of a RP KAT

By default, the default value of a keepalive timer (KAT) is used. The default value is calculated as follows: Suppression time of a register packet x 3 + Inspection time of a null register packet.

Run **ip pim rp-register-kat seconds** to configure the KAT time.

You can run this command if you want to configure the keepalive time of (S, G) of a register packet sent from an RP.

6.3.6 Creating an RPT

When a group member is detected on the network, the DR connecting to the group members send packets toward the RP to form an RPT. If the multicast source already exists on the network, the packets arrived at the RP can be sent to the group members along the RPT.

Working Principle

To create an RPT, perform the following steps:

- 1) A receiver DR receives an IGMP (*, G) include report packet from the receiving end.
- 2) If the DR is not the RP of this group (G), the DR will send a (*, G) Join packet toward the RP. The router receiving this (*, G) Join packet will send the packet hop by hop until it is received by the RP, which means that the RP has joined the RPT.
- 3) When the data source host sends the multicast data to a group, the source data is encapsulated in the register packet, and sent from the source DR to the RP in unicast mode. Then the RP decapsulates the register packet, takes the data packets out, and forwards these packets to each group member along the RPT.

- 4) The RP sends the (S, G) Join packets along the data source to join the SPT of this source.
- 5) After the SPT between the RPs to the source DR is created, the data packets from the data source will be sent decapsulated to the RPs along the SPT.
- 6) When the first multicast data packet arrives at an RP along the SPT, the RP sends a Register-Stop packet to the source DR to stop sending a register packet. After the source DR receives the Register-Stop packet, it stops encapsulating a register packet and sends the packet along the SPT to the RP, which will forwards the packet to each group member.

Related Configuration

❖ Configuring the Interval for Sending a Join/Prune Packet

By default, the interval for sending a Join/Prune packet is 60s.

Run **ip pim jp-timer seconds** to configure the interval for sending a Join/Prune packet.

You can run this command to configure the interval for sending a Join/Prune packet. If not configured, the value will be a default 60s.

6.3.7 Creating an SPT

When data packets arrive at the DR connecting to group members, the DR sends these packets toward the multicast source to form an SPT, and multicast packets are sent to group members along the SPT. In this way, the burden on RP in the RPT is reduced, and the source DR will arrive at the receiver DR with less hops.

Working Principle

To create an SPT, perform the following steps:

- 7) The receiver DR sends (*, G) Join packets toward the source DR along the SPT, and (*, G) Join packets are then send hop by hop until they are received by the source DR, forming an SPT.

Related Configuration

By default, SPT switchover is not enabled.

Run **ip pim spt-threshold [group-list access-list]** to configure whether to switch to an SPT.

If this function is enabled, upon the reception of the first (S, G) packet, a PIM Join packet is triggered, and an SPT is created. If **group-list** is specified, all the specified groups will be switched to the SPT. If the **no** form of this command is used and **group-list** is not specified, an RPT will not be switched to an SPT, and the DR will remain in the RPT and send a Prune packet toward the source DR; if the **no** form of this command is used and **group-list** is specified, and that the ACLs have been configured, it means that the association between **group-list** and the ACLs is canceled, and all the groups are allowed to switch from an RPT to an SPT.

6.3.8 ASM and SSM

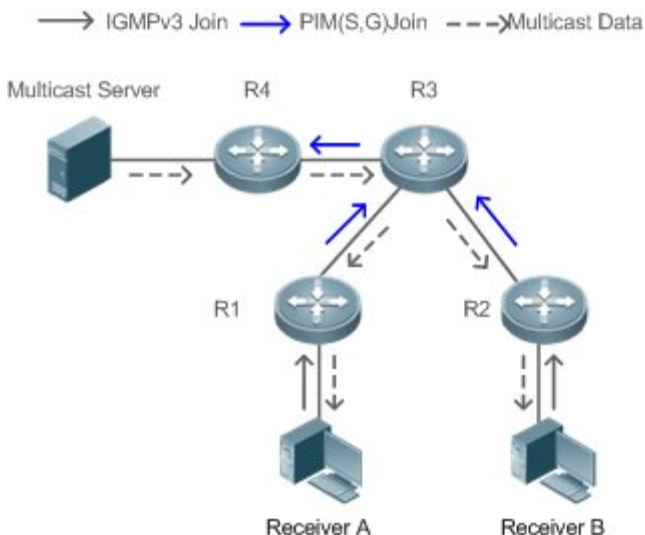
A PIM router can provide multicast services of both ASM model and SSM model at the same time. SSM model applies to the groups whose addresses are within the range of the SSM addresses. For other groups, use ASM model. In an ASM model, only the multicast group (G) is specified for a multicast receiver, and the multicast source (S) is not specified. In an SSM model, both the multicast source (S) and multicast group (G) can be specified for a multicast receiver.

Working Principle

To realize SSM in an IPv4 router, IGMPv3 needs to be applied for managing membership between the host and devices, and PIM-SM needs to be applied to connect to devices.

In an SSM model, as a multicast receiver has learnt the (S, G) of the multicast source through a certain channel (for example, by visiting the server or receiving an advertisement), when a multicast receiver needs to request a multicast service, the multicast receiver can send the IGMP (S, G) Join packet toward the router of last hop. For example, as shown in Figure 1-3, the multicast receiver 1 sends the IGMP (S, G) Join packet to request the multicast service (S, G). After the router of last hop receives the IGMP (S, G) Join packet, it sends the PIM (S, G) Join packet to the multicast source hop by hop. As shown in Figure 6-4, when R 1 receives the IGMP (S, G) Join packet sent from multicast Receiver 1, R 1 sends the PIM (S, G) Join packet to R 3, which then sends the packet to R 4, thereby forming an SPT connecting the multicast receiver and multicast source.

Figure 6-4 SSM Model



To create an SSM model, the following requirements need to be met:

- A multicast receiver needs to learn the (S, G) of the multicast source in advance, and an IGMP (S, G) Join packet needs to be sent if the receiver needs to request a multicast service.
- IGMPv3 must be run on the interface of the last hop router connecting to the multicast receiver. IGMPv1 and IGMPv2 does not support SSM.

- PIM-SM and SSM must be run on the devices connecting the multicast receiver and multicast source.

The default range of SSM groups is 232/8. You can run a command to change the value.

An SSM has the following features:

- A multicast receiver can learn the information of the multicast source through a certain channel (for example, by visiting the server or receiving an advertisement) in advance.
- An SSM model is a specific subnet of PIM-SM. It handles only the PIM (S, G) Join and PIM (S, G) Prune packets and discards the RPT-related packets, for example, PIM (*, G) Join/Prune packets, that are within the scope the SSM. If the SSM detects a register packet within the scope, it will respond immediately with a Register-Stop packet.
- If an RP is not required, the election and distribution of RP information are not performed. The MDTs in an SSM are all SPTs.

Related Configuration

ASM is enabled by default.

Run `ip pim ssm { default | range access-list }` to configure whether to switch to SSM.

In SSM, multicast packets can be received by the multicast source directly but not along the RP tree.

6.4 Configuration

Configuration	Description and Command	
Configuring Basic PIM-SM Functions	(Mandatory) It is used to configure the multicast service.	
	<code>ip multicast-routing</code>	Enables IPv4 multicast routing.
	<code>ip pim sparse-mode</code>	Enables PIM-SM.
	<code>ip pim rp-address</code>	Configures a static RP.
	<code>ip pim rp-candidate</code>	Configures a C-RP.
	<code>ip pim bsr-candidate</code>	Configures a C-BSR.
Configuring PIM-SM Neighbors	(Optional) It is used to configure the parameters for sending and receiving the Hello packets between neighbors.	
	<code>ip pim query-interval interval-seconds</code>	Configures the interval for sending Hello packets.
	<code>ip pim propagation-delay milliseconds</code>	Configures the prune propagation delay.
	<code>ip pim override-interval milliseconds</code>	Configures the prune override interval.
	<code>ip pim neighbor-tracking</code>	Enables the suppression capability of an interface for sending Join packets.

Configuration	Description and Command	
	ip pim triggered-hello-delay <i>interval-seconds</i>	Configures the delay for sending Hello packets.
	ip pim dr-priority <i>priority-value</i>	Configures the DR priority of a Hello packet.
	ip pim neighbor-filter <i>access_list</i>	Configures neighbor filtering.
Configuring BSR Parameters	(Optional) It is used to configure a BSR.	
	ip pim bsr-border	Configures BSR borders.
	ip pim accept-bsr list { <1-99> <1300-1999> <i>WORD</i> }	Configures BSM packets limit on a PIM router.
	ip pim accept-crp list <i>access-list</i>	Configures a C-BSR to inspect the address range of a C-PR.
Configuring RP and DR Parameters	(Optional) It is used to configure the parameters of an RP or a DR.	
	ip pim ignore-rp-set-priority	Ignores the C-RP priority.
	ip pim register-rp-reachability	Enables the source DR to detect the RP reachability.
	ip pim accept-register list <i>access-list</i>	Configures the range of source register (S, G) addresses.
	ip pim register-rate-limit <i>rate</i>	Limits the speed for sending register packets.
	ip pim register-checksum-wholepkt [<i>group-list</i> <i>access-list</i>]	Calculates the checksum of the entire register packet.
	ip pim register-decapsulate-forward	Enables an RP to decapsulate a register packet and forwards the multicast packet to interfaces.
	ip pim register-source { <i>local_address</i> <i>Interface-type interface-number</i> }	Configures the source IP address of a register packet.
	ip pim register-suppression <i>seconds</i>	Configures the suppression time of a register packet.
	ip pim probe-interval <i>seconds</i>	Configures the inspection time of a null register packet.
	ip pim rp-register-kat <i>seconds</i>	Configures the interval of KATs on an RP.
Configuring the Interval for Sending a Join/Prune Packet	(Optional) It is used to specify the interval for sending a Join/Prune packet.	
	ip pim jp-timer <i>seconds</i>	Configures the interval for sending a Join/Prune packet.

Configuration	Description and Command
Configuring the Router of Last Hop to Switch from an RPT to SPT	(Optional) It is used to switch from SPT to RPT.
	<pre>ip pim spt-threshold [group-list access-list]</pre> <p>Enables SPT switchover.</p>

6.4.1 Configuring Basic PIM-SM Functions

Configuration Effect

- Create a PIM-SM network and provide data sources and user terminals on the network with the IPv4 multicast service.
- Any of ASM or SSM or both models can be configured.

Notes

- PIM-SM needs to use existing unicast routes on the network. Therefore, IPv4 unicast routes must be configured on the network.
- If the PIM network needs to support SSM multicast services, IGMPv3 or SSM mapping must be configured.

Configuration Steps

- ❖ Enabling IPv4 Multicast Routing
 - Mandatory.
 - If not specified, IPv4 multicast routing must be enabled on each router.
- ❖ Enabling PIM-SM
 - Mandatory.
 - If not specified, PIM-SM must be enabled on the following interfaces: interconnecting router interfaces, interfaces of static RPs, C-RPs, and C-BSRs, and the interfaces connecting to the multicast source and user hosts.
- ❖ Configuring an RP
 - An RP must be configured if ASM multicast services need to be provided on a PIM network.
 - An RP can be configured in three models: configuring only a static RP, configuring only a dynamic RP, and configuring both a static RP and dynamic RP. If both a static RP and dynamic RP are configured, the dynamic RP takes precedence over the static RP.
 - Configuring a static RP: If not specified, a static RP should be configured on each router.
 - Configuring a dynamic RP: If not specified, a C-RP and C-BSR should be configured on one or multiple routers.
- ❖ Enabling SSM

- SSM must be enabled if SSM multicast services need to be provided on a PIM network.
- If not specified, SSM must be enabled on every router.

Verification

Send multicast packets from the multicast source to the groups within the address range of ASM and SSM, and join user hosts to these groups.

- Check whether the user hosts can successfully receive packets from each group.
- Check whether PIM-SM routing entries are created on routers correctly.

Related Commands

❖ Enabling IPv4 Multicast Routing

Command	ip multicast-routing
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Enabling PIM-SM

Command	ip pim sparse-mode
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	PIM interfaces must be at Layer-3, including: routing interfaces, aggregate ports (APs), switch virtual interfaces (SVIs), and loopback interfaces. For all PIM interfaces, IPv4 unicast routes should be reachable.

❖ Configuring a Static RP

Command	ip pim rp-address <i>rp-address</i> [<i>access_list</i>]
Parameter Description	<i>rp-address</i> : Indicates the address of an RP. <i>access_list</i> : Specifies the range of multicast group addresses served by a static RP using an ACL. By default, an RP services all groups.
Command Mode	Global configuration mode
Usage Guide	This command is used to locate a static RP. A static RP should be one with good routing performance. It is recommended that the address of the loopback interface be used as the static RP address.

	<p>The static RP of all routers must be the same (including the RP address and the range of multicast group addresses it serves). It is recommended that the address of the loopback interface be used as the static RP address.</p> <p>The load can be shared if you configure multiple static RPs to serve different multicast group addresses. It is recommended that the address of the loopback interface be used as the static RP address.</p>
--	--

❖ Configuring a C-RP

Command	ip pim rp-candidate <i>interface-type interface-number</i> [priority <i>priority-value</i>] [interval <i>seconds</i>] [group-list <i>access_list</i>]
Parameter Description	<p><i>interface-type interface-number</i>: Uses the address of this interface as the address of the C-RP.</p> <p>priority <i>priority-value</i>: Competes for the RP priority. A greater value indicates a higher priority. The value ranges from 0 to 255 (192 by default).</p> <p>interval <i>seconds</i>: Indicates the interval for sending a C-RP packet to a BSR. The value ranges from 1 to 16,383 (60 by default).</p> <p>group-list <i>access_list</i>: Specifies the range of multicast group addresses served by a C-RP using an ACL. By default, a C-RP services all multicast groups.</p>
Command Mode	Global configuration mode
Usage Guide	<p>This command is used to configure a router as a C-RP.</p> <p>A C-RP should be one with good routing performance. A C-RP and C-BSR can be on the same router or different routers.</p> <p>It is recommended that the address of the loopback interface be used as the C-RP address.</p> <p>If multiple C-RPs serve the same group, redundancy can be realized.</p> <p>If multiple C-RPs serve the different groups, load can be shared.</p>

❖ Configuring a C-BSR

Command	ip pim bsr-candidate <i>interface-type interface-number</i> [<i>hash-mask-length</i> [<i>priority-value</i>]]
Parameter Description	<p><i>interface-type interface-number</i>: Uses the address of this interface as the address of the C-BSR.</p> <p><i>hash-mask-length</i>: Indicates the length of hash mask used to competing for the RP. The value ranges from 0 to 32 (10 by default).</p> <p><i>priority-value</i>: Indicates the priority for competing for the BSR. A greater value indicates a higher priority. The value ranges from 0 to 255 (64 by default).</p>
Command Mode	Global configuration mode
Usage Guide	<p>This command is used to configure a router as a C-BSR.</p> <p>A C-BSR should be one with good routing performance. A C-RP and C-BSR can be on the same router or different routers.</p> <p>It is recommended that the address of the loopback interface be used as the C-BSR address.</p> <p>Configuring multiple C-BSRs can realize redundancy.</p>

❖ Enabling SSM

Command	ip pim ssm { default range <i>access_list</i> }
----------------	--

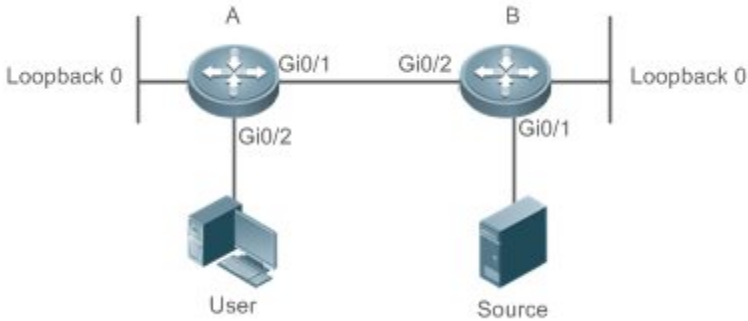
Parameter Description	default: Indicates the default range of SSM group addresses, which is 232.0.0.0/8. range access_list: Specifies the range of SSM group addresses using an ACL.
Command Mode	Global configuration mode
Usage Guide	The SSM group addresses configured on all routers must be the same.

❖ Displaying the PIM-SM Routing Entry

Command	show ip pim sparse-mode mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]] [proxy]
Parameter Description	<i>group-or-source-address:</i> Indicates a multicast group address or source address (the two addresses cannot be multicast group addresses or source addresses at the same time). proxy: Indicates the RPF vector carried by an entry.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	Check whether sufficient routing entries are provided. Check the upstream and downstream interface lists and ensure that a correct SPT tree is created.

Configuration Example

❖ Enabling IPv4 Multicast Routing to Support ASM and SSM

Scenario	Figure 6-5 
Configuration Steps	<ul style="list-style-type: none"> ➤ Configure a IPv4 unicast routing protocol (such as OSPF) on a router, and the router is reachable for the unicast route of a loopback interface. (Omitted) ➤ Enable IPv4 multicast routing on all the routers. ➤ Enable PIM-SM on all the interconnected interfaces of the routers, Source, and Receiver. ➤ Configure C-RP and C-BSR on the loopback interfaces of Router A and Router B, and enable PIM-SM on the loopback interfaces. ➤ Enable SSM on all routers. ➤ Enable IGMPv3 on the router interfaces connecting to user terminals. (Omitted)
A	<pre>A# configure terminal A(config)# ip multicast routing</pre>

	<pre>A(config)# ip pim ssm default A(config)# interface GigabitEthernet 0/1 A(config if)# ip pim sparse mode A(config if)# exit A(config)# interface GigabitEthernet 0/2 A(config if)# ip pim sparse mode A(config if)# exit A(config)# interface loopback 0 A(config if)# ip pim sparse mode A(config if)# exit A(config)# ip pim rp candidate loopback 0</pre>
B	<pre>B# configure terminal B(config)# ip multicast routing B(config)# ip pim ssm default B(config)# interface GigabitEthernet 0/1 B(config if)# ip pim sparse mode B(config if)# exit B(config)# interface GigabitEthernet 0/2 B(config if)# ip pim sparse mode B(config if)# exit B(config)# interface loopback 0 B(config if)# ip pim sparse mode B(config if)# exit B(config)# ip pim bsr candidate loopback 0</pre>
Verification	<p>Send packets from S (192.168.1.10) to G 1 (229.1.1.1) and G2 (232.1.1.1). Add the user to G 1 and G 2, and specify the source when the user joins G 2.</p> <ul style="list-style-type: none"> ➤ Check that multicast packets from S (192.168.1.10) to G 1 and G 2 are received by the user. ➤ Check the PIM-SM routing entries on Router A and Router B. Entries (*, 229.1.1.1), (192.168.1.10, 229.1.1.1), and (192.168.1.10, 232.1.1.1) should be displayed.
A	<pre>switch#show ip pim sparse mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0</pre>


```

Upstream State: JOINED

jt_timer expires in 8 seconds
kat expires in 207 seconds

 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31

Local
0 . . . . .
. . . . .
1 . . . . .
. . . . .

Joined
0 . . . . .
. . . . .
1 . . . . .
. . . . .

Asserted
0 . . . . .
. . . . .
1 . . . . .
. . . . .

Outgoing
0 . . .
o . . . . .
. . .
1 . . . . .
. . . . .

(192.168.1.10, 229.1.1.1, rpt)
RP: 192.168.10.10
RPF nbr: 0.0.0.0
RPF idx: None

Upstream State: PRUNED

 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31

Local

```

```
0 . . . . .
. . . . .
1 . . . . .
. . . . .

Pruned
0 . . . . .
. . . . .
1 . . . . .
. . . . .

Outgoing
0 . . .
0 . . . . .
. . .
1 . . . . .
. . . . .

(*, 232.1.1.1)
RP: 192.168.10.10
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31

Local
0 . . .
i . . . . .
. . .
1 . . . . .
. . . . .

Joined
0 . . . . .
. . . . .
1 . . . . .
. . . . .

Asserted
```

```
0 . . . . .
. . . . .
1 . . . . .
. . . . .
FCR:
(192.168.1.10, 232.1.1.1)
RPF nbr: 192.168.2.1
RPF idx: GigabitEthernet 0/2
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 8 seconds
kat expires in 207 seconds
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31
Local
0 . . . . .
. . . . .
1 . . . . .
. . . . .
Joined
0 . . . . .
. . . . .
1 . . . . .
. . . . .
Asserted
0 . . . . .
. . . . .
1 . . . . .
. . . . .
Outgoing
0 . . .
o . . . . .
. . .
1 . . . . .
. . . . .
```

```
(192.168.1.10, 232.1.1.1, rpt)
RP: 192.168.10.10
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: PRUNED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
  22 23 24 25 26 27 28 29 30 31
Local
0 . . . . .
. . . . .
1 . . . . .
. . . . .
Pruned
0 . . . . .
. . . . .
1 . . . . .
. . . . .
Outgoing
0 . . .
o . . . . .
. . .
1 . . . . .
. . . . .
(*, 239.255.255.250)
RP: 192.168.10.10
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
  22 23 24 25 26 27 28 29 30 31
Local
0 . . .
i . . . . .
. . .
1 . . . . .
. . . . .
```

	<pre> Joined 0 . j 1 Asserted 0 1 FCR: A# </pre>
<p>B</p>	<pre> B#show ip pim sparse mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 1 (192.168.1.10, 229.1.1.1) RPF nbr: 0.0.0.0 RPF idx: None SPT bit: 1 Upstream State: JOINED kat expires in 38 seconds 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 </pre>

```
Joined
0 . .
j . . . . .
. . . . .

Asserted
0 . . . . .
. . . . .

Outgoing
0 . .
o . . . . .
. . . . .

(192.168.1.10, 229.1.1.1, rpt)
RP: 192.168.10.10
RPF nbr: 192.168.2.2
RPF idx: GigabitEthernet 0/2
Upstream State: RPT NOT JOINED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31

Local
0 . . . . .
. . . . .

Pruned
0 . . . . .
. . . . .

Outgoing
0 . . . . .
. . . . .

(192.168.1.10, 232.1.1.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
kat expires in 38 seconds
```

```
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31

Local
0 . . . . .
. . . . .

Joined
0 . .
j . . . . .
. . . . .

Asserted
0 . . . . .
. . . . .

Outgoing
0 . .
o . . . . .
. . . . .

(192.168.1.10, 232.1.1.1, rpt)
RP: 192.168.10.10
RPF nbr: 192.168.2.2
RPF idx: GigabitEthernet 0/2
Upstream State: RPT NOT JOINED

 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31

Local
0 . . . . .
. . . . .

Pruned
0 . . . . .
. . . . .

Outgoing
0 . . . . .
. . . . .

(*, 239.255.255.250)
RP: 192.168.10.10
RPF nbr: 192.168.2.2
```

```

RPF idx: GigabitEthernet 0/2
Upstream State: JOINED
jt_timer expires in 15 seconds
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31

Local
0 .
i . . . . .
. . . . .

Joined
0 . . . . .
. . . . .

Asserted
0 . . . . .
. . . . .

FCR:
    
```

Common Errors

- IPv4 unicast routing is incorrectly configured.
- IPv4 multicast routing is not enabled on a certain router.
- SSM is not enabled on a router or the SSM group address is different from that of the others'.
- PIM-SM is not enabled on an interface (for example, the interface is configured as a C-RP or C-BSR interface, or is used to connecting to the user host or used as an interface of the multicast source).
- IGMPv3 is not enabled on an interface connecting to the used host.
- RP is not configured on the network.
- A static RP is not configured on a router, or the configured static RP is different from that on other routers.
- C-RPs are configured on the network, but C-BSRs are not.
- Static RPs, C-RPs or C-BSRs are unreachable for unicast routes.

6.4.2 Configuring PIM-SM Neighbors

Configuration Effect

- Coordinate protocol parameters and adjust parameters in the Hello packet.

- A RIM router is used to discover neighbors, coordinate protocol parameters, and maintain neighbor relationships.
- Maintain neighbor relationships and filter the neighbors.

Notes

- Basic PIM-SM functions must be configured.

Configuration Steps

- Configure parameters on PIM router interfaces If not specified.

Verification

Configure the parameters of a Hello packet sent from an interface and run **debug ip pim sparse-mode packet** to display the parameters.

Enable neighbor filtering and run **show ip pim sparse-mode neighbor** to display neighbor information.

Related Commands

❖ Configuring the Interval for Sending Hello Packets

Command	ip pim query-interval <i>interval-seconds</i>
Parameter Description	Indicates the interval for sending Hello packets, Indicates the suppression time of a register packet in the unit of seconds. The value ranges from 1 to 65,535 (30 by default).
Command Mode	Interface configuration mode
Usage Guide	Every time when the interval for sending Hello packets is updated, the holdtime value is automatically updated as 3.5 times of the interval. If the result of the interval for sending Hello packets multiplied by 3.5 is greater than 65, 535, the holdtime value is forcibly updated as 18,725.

❖ Configuring the Prune Propagation Delay

Command	ip pim propagation-delay <i>milliseconds</i>
Parameter Description	<i>milliseconds</i> : The unit is ms. The value ranges from 1 to 32,767 (500 by default).
Command Mode	Interface configuration mode
Usage Guide	Once the prune propagation delay or prune override interval is changed, the Join/Prune packet override interval will be changed. As specified by the protocol, the Join/Prune packet override interval must be smaller than the holdtime of a Join/Prune packet; otherwise, short break-up of traffic may be caused. The administrator should maintain such configuration.

❖ Configuring the Prune Override Interval

Command	ip pim override-interval <i>milliseconds</i>
----------------	---

Parameter Description	<i>milliseconds</i> : The unit is ms. The value ranges from 1 to 65,535 (2,500 by default).
Command Mode	Interface configuration mode
Usage Guide	Once the prune propagation delay or prune override interval is changed, the Join/Prune packet override interval will be changed. As specified by the protocol, the Join/Prune packet override interval must be smaller than the holdtime of a Join/Prune packet; otherwise, short break-up of traffic may be caused. The administrator should maintain such configuration.

❖ Enabling Suppression Capability of an Interface for Sending Join Packets

Command	ip pim neighbor-tracking
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Once Join packets suppression of an interface is enabled, when the present router is to send a Join packet to the upstream neighbor, which has sent a Join packet to its own upstream neighbor, the present router will not send the Join packet; if Join packets suppression is disabled, the Join packet will be sent. When Join packets suppression from downstream receivers are disabled, upstream neighbors will learn how many downstream neighbors are there by counting the Join packets it received, which is called neighbor tracking.

❖ Configuring the Delay for Sending Hello Packets

Command	ip pim triggered-hello-delay <i>interval-seconds</i>
Parameter Description	<i>Seconds</i> : The unit is second. The value ranges from 1 to 5 (5 by default).
Command Mode	Interface configuration mode
Usage Guide	When a PIM interface is enabled or detects a new neighbor, a triggered-hello-delay packet is used to generate a random time. Within the time, the interface sends Hello packets.

❖ Configuring the DR Priority of a Hello Packet

Command	ip pim dr-priority <i>priority-value</i>
Parameter Description	<i>priority-value</i> : Indicates the priority. A greater value indicates a higher priority. The value ranges from 0 to 4,294,967,294 (1 by default).
Command Mode	Interface configuration mode
Usage Guide	A DR may be selected based on the following principles: If all the Hello packets sent from the routers on a local area network (LAN) are configured with priorities, when selecting a DR, the priorities will be compared, and the router with the highest priority will be selected as the DR. If the priority of all routers is the same, their IP addresses will be compared, and the router with the maximum IP address will be selected as the DR.

	If the priority of the Hello packets sent from a certain router is not configured, the IP addresses of the routers will be compared, and the router with the maximum IP address will be selected as the DR.
--	---

❖ Configuring Neighbor Filtering

Command	ip pim neighbor-filter <i>access_list</i>
Parameter Description	<i>access_list</i> : Configures the range of neighbor addresses using a standard IP ACL. The value can be set from 1 to 99 or a string.
Command Mode	Interface configuration mode
Usage Guide	Enabling neighbor filtering can enhance the security of the PIM network and limit the range of legible neighbor addresses. Once a neighbor is filtered out, PIM-SM will not establish peering with it or stop the peering with it.

❖ Displaying the Neighbor Information of an Interface

Command	show ip pim sparse-mode neighbor [detail]
Parameter Description	detail : Displays detailed information.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ Configure the interval for sending Hello packets as 50s. ➤ Configure the prune propagation delay as 400 ms. ➤ Configure the prune override interval as 3,000 ms. ➤ Enable suppression capability of an interface for sending Join packets. ➤ Configure the delay for sending Hello packets as 3s. ➤ Configure the DR priority of a hello packet as 5.
	<pre>Qtech# configure terminal Qtech (config)#int gi 0/1 Qtech (config if GigabitEthernet 0/1)#ip pim query interval 50 Qtech (config if GigabitEthernet 0/1)#ip pim propagation delay 400 Qtech (config if GigabitEthernet 0/1)#ip pim override interval 3000 Qtech (config if GigabitEthernet 0/1)#ip pim triggered hello delay 3 Qtech (config if GigabitEthernet 0/1)#ip pim neighbor tracking</pre>
Verification	Run debug ip pim sparse-mode packet to display the parameters of a Hello packet.
	<pre>Qtech# debug ip pim sparse mode packet</pre>

	<pre>00:01:49:43: %7: VRF(0): Hello send to GigabitEthernet 0/1 00:01:49:43: %7: Send Hello packet 00:01:49:43: %7: Holdtime: 175 00:01:49:43: %7: T bit: on 00:01:49:43: %7: Propagation delay: 400 00:01:49:43: %7: Override interval: 3000 00:01:49:43: %7: DR priority: 5 00:01:49:43: %7: Gen ID: 355154648 00:01:49:43: %7: RPF Vector capable</pre>
Configuration Steps	Configure neighbor filtering and set the allowed address range to 192.168.1.0 to 192.168.1.255.
	<pre>Qtech# configure terminal Qtech (config)#int gi 0/1 Qtech (config if GigabitEthernet 0/1)# ip pim neighbor filter 1 % access list 1 not exist Qtech(config)# access list 1 permit 192.168.1.0 0.0.0.255 Qtech(config)#</pre>
Verification	Display neighbor information before neighbor filtering is configured.
	<pre>Qtech# show ip pim sparse mode neighbor Neighbor Interface Uptime/Expires Ver DR Address Priority/Mode 192.168.36.89 GigabitEthernet 0/1 01:12:13/00:01:32 v2 1 / P</pre>
	Display neighbor information after neighbor filtering is configured.
	<pre>Qtech# show ip pim sparse mode neighbor</pre>

Common Errors

- Basic PIM-SM functions are not configured or the configuration is not successful.

6.4.3 Configuring BSR Parameters

Configuration Effect

- Configure the address range of BSM packets.

Notes

- Basic PIM-SM functions must be configured.
- C-RPs and C-BSRs must be configured.
- Borders must be configured on the interfaces between domains.

Configuration Steps

- ❖ Configuring Borders
 - Borders must be configured if there are multiple domains.
 - Borders are configured on the interfaces separating two domains.
- ❖ Configuring BSM Packets Limit on a PIM Router
 - Optional.
 - If not specified, BSM packets limit can be configured on all PIM routers.
- ❖ Configuring a C-BSR to Inspect the Address Range of a C-PR
 - Optional.
 - If not specified, C-PR range inspection can be configured on all C-BSRs.
- ❖ Allowing a C-BSR to Receive a C-RP-ADV Packet Whose Prefix-Count Is 0
 - Optional.
 - If not specified, this function can be configured on all C-BSRs.

Verification

- ❖ Border Inspection

Enable basic PIM-SM functions. Configure two routers to be in different domains, configure Router B as the C-BSR, and Router A to receive BSM packets.

Configure the junction of Router A and Router B as the border so that Router A does not receive BSM packets.

- ❖ Configuring to Inspect BSM Packets Limit on a PIM Router

When basic PIM-SM functions are enabled, and Router B is set as the C-BSR, Router A can receive BSM packets. When the address range of C-BSRs are limited on Router A, BSM packets will not be received by Router A.

- ❖ Configuring a C-BSR to Inspect the Address Range of a C-PR

When basic PIM-SM functions are enabled, Router B is set as the C-BSR, and Router A as the C-RP, if the address range of the C-RPs is limited on C-BSR, Router B will not receive the packets sent from the C-RPs.

Related Commands

- ❖ Configuring BSR Borders

Command	ip pim bsr-border
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	To prevent BSM flooding, you can configure a BSR boarder on an interface, so that the BSM packets arriving at this interface will be discarded but not forwarded.

❖ Configuring BSM Packets Limit on a PIM Router

Command	ip pim accept-bsr list { <1-99> <1300-1999> WORD }
Parameter Description	list access-list: Configures the range of BSR addresses using a standard IP ACL. The value can be 1 to 99, 1,300 to 1,999, or a string.
Command Mode	Global configuration mode
Usage Guide	After this function is enabled, PIM-SM routers receive only the BSM packets sent from legible BSRs.

❖ Configuring a C-BSR to Inspect the Address Range of a C-PR

Command	ip pim accept-crp list access-list
Parameter Description	list access-list: Specifies the range of C-RP addresses and the multicast group addresses they serve using an extended IP ACL. The value can be 100 to 199, 2,000 to 2,699, or a string.
Command Mode	Global configuration mode
Usage Guide	This command should be configured on a C-BSR. When the C-BSR becomes a BSR, it can set the range of legible C-RP addresses and the range of multicast group addresses they serves.

❖ Displaying BSM Packets Information

Command	show ip pim sparse-mode bsr-router
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A

❖ Displaying the Packets of All RPs and the Multicast Group Addresses They Serve

Command	show ip pim sparse-mode rp mapping
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A

Configuration Example

❖ Configuring BSR Borders

<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ On Router A, configure the address of the C-RP as 192.168.8.8. ➤ On Router B, configure the address of the C-RP as 192.168.5.5, and the address of the C-BSR as 192.168.6.6. ➤ Configure a BSR border on the junction of Router A and Router B.
	<pre>Qtech# configure terminal Qtech(config)# int GigabitEthernet 0/1 Qtech(config-if GigabitEthernet 0/1)# ip pim bsr border Qtech(config)# end</pre>
<p>Verification</p>	<p>Before configuring the boarder, display the BSM information on Router A.</p>
	<pre>Qtech# show ip pim sparse mode bsr router PIMv2 Bootstrap information This system is the Bootstrap Router (BSR) BSR address: 192.168.6.6 Uptime: 01:14:25, BSR Priority: 64, Hash mask length: 10 Next bootstrap packet in 00:00:52 Role: Candidate BSR Priority: 64, Hash mask length: 10 State: Elected BSR Candidate RP: 192.168.8.8(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:06</pre>
	<p>Candidate RP: Indicates all the C-RPs configured on the existing router. It does not include the C-RPs configured on other routers.</p>
	<p>After the boarder is configured, display the BSM information on Router A.</p>
	<pre>Qtech# show ip pim sparse mode bsr router</pre>

❖ Configuring BSM Packets Limit on a PIM Router, Filtering BSM Source Addresses, and Configuring the Range of BSM Source Addresses to 192.168.1.1 to 192.168.1.255

<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ On Router A, configure the address of the C-RP as 192.168.8.8.
-----------------------------------	---

	<ul style="list-style-type: none"> ➤ On Router B, configure the address of the C-RP as 192.168.5.5, and the address of the C-BSR as 192.168.6.6. ➤ On Router A, configure the range of allowed BSM source addresses to 192.168.1.1 to 192.168.1.255.
	<pre>Qtech# configure terminal Qtech(config)# ip pim accept bsr list 1 % access list 1 not exist Qtech(config)# access list 1 permit 192.168.1.0 0.0.0.255 Qtech(config)#</pre>
Verification	<p>Before configuring BSM packets limit, display the BSM information on Router A.</p>
	<pre>Qtech#show ip pim sparse mode bsr router PIMv2 Bootstrap information BSR address: 192.168.6.6 Uptime: 00:00:11, BSR Priority: 64, Hash mask length: 10 Expires: 00:01:59 Role: Non candidate BSR Priority: 0, Hash mask length: 10 State: Accept Preferred Candidate RP: 192.168.8.8(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:06</pre>
	<p>After BSM packets limit is configured, display the BSM information on Router A.</p>
	<pre>Qtech# show ip pim sparse mode bsr router Candidate RP: 192.168.8.8(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:06</pre>

❖ **Configuring a C-BSR to Inspect the Address Range of a C-PR, Filtering C-RP Addresses, and Configuring the Range of C-RP Addresses to 192.168.1.1 to 192.168.1.255**

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ On Router A, configure the address of the C-RP as 192.168.8.8. ➤ On Router B, configure the address of the C-RP as 192.168.5.5, and the address of the C-BSR as 192.168.6.6. ➤ On Router B, configure the range of allowed C-RP source addresses to 192.168.1.1 to 192.168.1.255.
----------------------------	--

	<pre>Qtech# configure terminal Qtech(config)# ip pim accept crp list 100 % access list 1 not exist Qtech(config)# access list 1 permit 192.168.1.0 0.0.0.255 Qtech(config)#</pre>
Verification	Before configuring C-RP filtering, display the information of all RP groups on Router B.
	<pre>Qtech#show ip pim sparse mode rp mapping PIM Group to RP Mappings This system is the Bootstrap Router (v2) Group(s): 224.0.0.0/4 RP: 192.168.8.8(Not self) Info source: 192.168.8.8, via bootstrap, priority 192 Uptime: 00:15:16, expires: 00:02:18 RP: 192.168.5.5(Self) Info source: 192.168.6.6, via bootstrap, priority 192 Uptime: 18:52:30, expires: 00:02:00</pre>
	After C-RP filtering is configured, display the information of all RP groups on Router B.
	<pre>Qtech#show ip pim sparse mode rp mapping PIM Group to RP Mappings This system is the Bootstrap Router (v2) Group(s): 224.0.0.0/4 RP: 192.168.5.5(Self) Info source: 192.168.6.6, via bootstrap, priority 192 Uptime: 21:38:20, expires: 00:02:10</pre>
	After C-RP filtering is configured on a router, only the C-RP packets sent from other routers are filtered, and those sent from the present router are not filtered.

Common Errors

- Basic PIM-SM functions are not configured or the configuration is not successful.
- C-BSRs are not configured.
- The BSR border is not configured on the interfaces of different domains.

6.4.4 Configuring RP and DR Parameters

Configuration Effect

- Ignore the C-RP priority and reselect an RP.
- Detect the reachability of an RP for the source DR.
- Configure the range of (S, G) addresses of source register packets, and allow the ASM to serve only the multicast packets within the range.
- Limit the speed of the source DR for sending register packets.
- Configure the checksum of the register packet length.
- Configure an RP to decapsulate register packets and forward the multicast packets to downstream interfaces.
- Configure the source IP address of a register packet.
- Configure the suppression time of a register packet.
- Configure the inspection time of a null register packet.
- Configure the (S, G) lifetime based on the register packet received by an RP.

Notes

- Basic PIM-SM functions must be configured.

Configuration Steps

- ❖ Ignoring the C-RP Priority and Reselecting an RP
 - Optional.
 - If not specified, the C-RP priority can be disabled on every router.
- ❖ Detecting the Reachability of an RP for the Source DR
 - Optional.
 - If not specified, this function can be enabled on the DR connected directly to the data source.
- ❖ Configuring the Range of Source Register (S, G) Addresses
 - Optional.
 - If not specified, source register address filtering can be enabled on all C-RPs or static RPs.
- ❖ Limiting the Speed of the Source DR for Sending Register Packets
 - Optional.
 - If not specified, this function can be enabled on the source DR.
- ❖ Configuring the Checksum of the Register Packet Length
 - Optional.
 - If not specified, this function can be enabled on all C-RPs or static RPs.

- ❖ Configuring Whether to Forward the Multicast Packet After Decapsulating a Register Packet
 - Optional.
 - If not specified, this function can be enabled on all C-RPs or static RPs.
- ❖ Configuring the Source IP Address of a Register Packet
 - Optional.
 - If not specified, the source IP address of a register packet can be configured on the DR connected directly to the data source.
- ❖ Configuring the Suppression Time of a Register Packet
 - Optional.
 - If not specified, the suppression time of a register packet can be configured on the DR connected directly to the data source.
- ❖ Configuring the Inspection Time of a Null Register Packet
 - Optional.
 - If not specified, the inspection time of a null register packet can be configured on the DR connected directly to the data source.
- ❖ Configuring the (S, G) Lifetime Based on the Register Packet Received by an RP
 - Optional.
 - If not specified, the (S, G) lifetime can be configured on all C-RPs or static RPs.

Verification

- ❖ Ignoring the C-RP priority

On Router A, configure the C-RP address as 192.168.8.8, and default priority as 192. On Router B, configure the C-RP address as 192.168.5.5, priority as 200, and C-BSR address as 192.168.6.6.

- Run **show ip pim sparse-mode rp 233.3.3.3** to display the RPs of the present group.

- ❖ Enabling the Source DR to Detect RP Reachability

On Router A, configure the C-RP address as 192.168.8.8, and default priority as 192. On Router B, configure the C-RP address as 192.168.5.5, priority as 192, and C-BSR address as 192.168.6.6. Enable Router B to detect RP reachability.

- Run **show running-config** to check whether the preceding configurations take effect.

- ❖ Configuring the Range of Source Register (S, G) Addresses

On Router A, configure the C-RP address as 192.168.8.8, and default priority as 192. On Router B, configure the address of the C-BSR as 192.168.6.6. Configure the source address a 192.168.1.100

and the multicast group address as 233.3.3.3. On Router A, configure the range of allowed source multicast group addresses to 192.168.2.0 to 192.168.2.255.

➤ Run **show ip pim sparse-mode mroute** to display the (S, G) entry.

❖ Limiting the Speed of the Source DR for Sending Register Packets

Configure the speed of Router B for sending register packets, and run **show ip pim sparse-mode track** to display the number of packets that has been sent.

❖ Configuring the Checksum of the Register Packet Length

On Router A, configure to calculate the checksum of the entire register packet length but not just the packet header. Run **show running-config** to check the configuration.

❖ Forwarding an RP Register Packet After It Is Decapsulated

On Router A, configure to forward a register packet after it is decapsulated. Run **show running-config** to display the configuration.

❖ Configuring the Source IP Address of a Register Packet

Configure the source address of a register packet on Router B, and run **show running-config** to display the configuration.

❖ Configuring the Suppression Time of a Register Packet and the Inspection Time of a Null Register Packet

On Router B, configure the suppression time and inspection time of a register packet, and run **show ip pim sparse-mode track** to display the configuration.

❖ Configuring an RP to Receive Register Packets and the (S, G) Lifetime

On Router A, configuring an RP to receive register packets and the (S, G) lifetime, and run **show ip pim sparse-mode mroute** to display the maximum (S, G) lifetime.

Related Commands

❖ Ignoring the C-RP priority

Command	ip pim ignore-rp-set-priority
Parameter	N/A
Description	
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Displaying the RP Corresponding to a Group

Command	show ip pim sparse-mode rp-hash group-address
---------	--

Parameter Description	<i>group-address</i> : Indicates the parsed multicast group address.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	N/A

❖ Enabling the Source DR to Detect RP Reachability

Command	ip pim register-rp-reachability
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After this function is enabled, the source DR will detect the RP reachability before sending a register packet. If the RP is unreachable, the packet will not be sent.

❖ Configuring the Range of Source Register (S, G) Addresses

Command	ip pim accept-register { list <i>access-list</i> [route-map <i>map-name</i>] route-map <i>map-name</i> [list <i>access-list</i>] }
Parameter Description	list <i>access-list</i> : Configures the range of (S, G) addresses using an extended IP ACL. The value can be 100 to 199, 2,000 to 2699, or a string. route-map <i>map-name</i> : Configures the range of (S, G) addresses using a route map.
Command Mode	Global configuration mode
Usage Guide	This command is run on a static RP or a C-RP to specify the source address and multicast group address of a register packet.

❖ Displaying a Multicast Routing Entry

Command	show ip pim sparse-mode mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]] [proxy]
Parameter Description	<i>group-or-source-address</i> : Indicates a multicast group address or source address (the two addresses cannot be multicast group addresses or source addresses at the same time). Proxy : Indicates the RPF vector carried by an entry.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	You can specify either a multicast group address or source address, or both a multicast group address and source address; or you can specify neither a multicast group address nor source address. The two addresses cannot be multicast group addresses or source addresses at the same time.

❖ Limiting the Speed of the Source DR for Sending Register Packets

Command	ip pim register-rate-limit <i>rate</i>
----------------	---

Parameter Description	<i>Rate</i> : Indicates the maximum number of register packets that can be sent each second. The value ranges from 1 to 65,535.
Command Mode	Global configuration mode
Usage Guide	This command takes effect for only the register packet of each (S, G) packet, but not all the register packets in the entire system. Enabling this command can reduce the burden on the source DR and RPs. Only the packets within the speed limit can be sent.

❖ Displaying the Counters of PIM-SM Packets

Command	show ip pim sparse-mode track
Parameter Description	N/A
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode
Usage Guide	The start time for counting PIM-SM packets is automatically enabled upon system startup. Run clear ip pim sparse-mode track to reset the start time and clear the PIM-SM packet counters.

❖ Calculating the Checksum of the Entire Register Packet Length

Command	ip pim register-checksum-wholepkt [group-list access-list]
Parameter Description	group-list access-list : Configures the multicast group addresses applicable to this configuration using an ACL. <i>access-list</i> : The value can be set to 1 to 99, and 1300 to 1999. It also supports the naming of the ACL.
Command Mode	Global configuration mode
Usage Guide	You can enable this function if you want to calculate the length of the entire PIM-SM packet, including that of the multicast packet encapsulated in the register packet, but not just the length of the PIM-SM packet header. If group-list access-list is specified, this configuration takes effect for all multicast group addresses.

❖ Enabling an RP to Decapsulate a Register Packet and Forward the Multicast Packet to Interfaces

Command	ip pim register-decapsulate-forward
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command is configured on a static RP or a C-RP. It is used to decapsulate a register packet with multicast packet and forward the multicast packet to interfaces. If there are too many register packets to be decapsulated, the CPU will be greatly burdened. In this case, this function is recommended to be disabled.

❖ Configuring the Source IP Address of a Register Packet

Command	ip pim register-source { local_address Interface-type interface-number }
----------------	---

Parameter Description	<i>local_address</i> : Specifies the source IP address of a register packet. <i>interface-type interface-number</i> : Specifies the IP address of this interface as the source IP address of the register packet.
Command Mode	Global configuration mode
Usage Guide	The specified address must be reachable. When an RP sends a Register-Stop packet, the PIM router corresponds to this address need to respond. Therefore, it is recommended that a loopback address (or other physical addresses) be used. This configuration does not require the enabling of PIM.

❖ Configuring the Suppression Time of a Register Packet

Command	ip pim register-suppression <i>seconds</i>
Parameter Description	<i>Seconds</i> : Indicates the suppression time of a register packet in the unit of seconds. The value ranges from 1 to 65,535 (60 by default).
Command Mode	Global configuration mode
Usage Guide	If you configure this parameter on a DR, the suppression time of a register packet sent from the DR will be changed. If ip pim rp-register-kat is not configured and if you configure this parameter on an RP, the RP keepalive will be changed.

❖ Configuring the Inspection Time of a Null Register Packet

Command	ip pim probe-interval <i>seconds</i>
Parameter Description	<i>Seconds</i> : Indicates the inspection time of a null register packet in the unit of seconds. The value ranges from 1 to 65,535 (5 by default).
Command Mode	Global configuration mode
Usage Guide	The inspection time of a null register packet indicates the period of time for sending a null register packet to an RP before the timeout of suppression time. The inspection time cannot exceed half of the suppression time; otherwise, the configuration will not take effect, and a warning message will be displayed. Meanwhile, the result of suppression time multiplied by 3 plus the inspection time cannot exceed 65,535, otherwise, a warning will be displayed.

❖ Configuring the Interval of KATs on an RP

Command	ip pim rp-register-kat <i>seconds</i>
Parameter Description	<i>Seconds</i> : Indicates the interval of a KAT in the unit of second. The value ranges from 1 to 65,535 (210 by default).
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

- ❖ Configuring the RPs of Corresponding Multicast Group Addresses When the C-RP Priority is Considered or Not Considered

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ On Router A, configure the address of the C-RP as 192.168.8.8. ➤ On Router B, configure the address of the C-RP as 192.168.5.5, priority as 200, and the address of the C-BSR as 192.168.6.6. ➤ Display the group corresponding to 233.3.3.3. ➤ Configure to ignore the C-RP priority on Router B.
	<pre>Qtech# configure terminal Qtech(config)# ip pim ignore rp set priority</pre>
Verification	Display the information before you configure to ignore the C-RP priority.
	<pre>Qtech# show ip pim sparse mode rp hash 233.3.3.3 RP: 192.168.8.8 Info source: 192.168.8.8, via bootstrap PIMv2 Hash Value 10(mask 255.192.0.0) RP 192.168.8.8, via bootstrap, priority 192, hash value 1084558102 RP 192.168.5.5, via bootstrap, priority 200, hash value 1094656709</pre>
	Display the information after you configure to ignore the C-RP priority.
	<pre>Qtech# show ip pim sparse mode rp hash 233.3.3.3 RP: 192.168.5.5 Info source: 192.168.6.6, via bootstrap PIMv2 Hash Value 10(mask 255.192.0.0) RP 192.168.8.8, via bootstrap, priority 192, hash value 1084558102 RP 192.168.5.5, via bootstrap, priority 200, hash value 1094656709</pre>

❖ Configuring to Inspect the Reachability of a Source RP

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ Configure to inspect the reachability of a source RP.
	<pre>Qtech(config)# ip pim register rp reachability</pre>
Verification	Run show running-config to check whether the following information is displayed.
	<pre>Qtech(config)#show running config ip pim register rp reachability</pre>

❖ Configuring the Range of Source Register (S, G) Addresses

<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ Configure source address filtering on Router A. The allowed address range is from 192.168.2.0 to 192.168.2.255.
	<pre>Qtech#show ip pim sparse mode mroute Qtech(config)#ip pim accept register list 101 % access list 101 not exist Qtech(config)#access list 101 permit ip 192.168.2.0 0.0.0.255 any Qtech#show ip pim sparse mode mroute</pre>
<p>Verification</p>	<p>Before enabling source address filtering, run show ip pim sparse-mode mroute to display the multicast entry, and check whether the (S, G) entry and (S, G, RPT) entry exist.</p>
	<pre>Qtech#show ip pim sparse mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 0 (192.168.1.100, 233.3.3.3) RPF nbr: 192.168.36.90 RPF idx: VLAN 1 SPT bit: 0 Upstream State: NOT JOINED kat expires in 187 seconds 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 Joined 0</pre>

```
Asserted
0 . . . . .
. . . . .

Outgoing
0 . . . . .
. . . . .

(192.168.1.100, 233.3.3.3, rpt)
RP: 192.168.8.8
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: RPT NOT JOINED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31

Local
0 . . . . .
. . . . .

Pruned
0 . . . . .
. . . . .

Outgoing
0 . . . . .
. . . . .

(*, 239.255.255.250)
RP: 192.168.8.8
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31

Local
0 . . . . .
. . . . .

Joined
```

	<pre> 0 . j Asserted 0 FCR: </pre>
	<p>After source address filtering is enabled, run show ip pim sparse-mode mroute to display the multicast entry, and check whether the (S, G) entry and (S, G, RPT) entry exist.</p>
	<pre> Qttech#show ip pim sparse mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 0 (S,G,rpt) Entries: 0 FCR Entries: 0 REG Entries: 0 (*, 239.255.255.250) RP: 192.168.8.8 RPF nbr: 0.0.0.0 RPF idx: None Upstream State: JOINED 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 Joined 0 . j Asserted </pre>

```
0 . . . . .
. . . . .
FCR:
```

❖ Limiting the Speed of the Source DR for Sending Register Packets

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ Check the number of PIM-SM packets sent by Router B. ➤ Check the number of PIM-SM packets sent by Router B in 1s. ➤ Configure the speed of Router B for sending register packets. ➤ Check the number of PIM-SM packets sent by Router B in 1s.
	<pre>Qtech (config)#ip pim register rate limit 1</pre>
Verification	<p>Display the number of PIM-SM packets sent by Router B before you configure the speed. The information should be displayed as follows:</p> <pre>Qtech#show ip pim sparse mode track PIM packet counters track Elapsed time since counters cleared: 04d01h01m received sent Valid PIM packets: 18754 29771 Hello: 11149 17842 Join Prune: 0 3234 Register: 0 3211 Register Stop: 3192 0 Assert: 0 0 BSM: 0 5484 C RP ADV: 4413 0 PIMDM Graft: 0 PIMDM Graft Ack: 0 PIMDM State Refresh: 0 Unknown PIM Type: 0 Errors: Malformed packets: 0 Bad checksums: 0</pre>

	<pre>Send errors: 0 Packets received with unknown PIM version: 0 Qtech#</pre>
	<p>Display the number of PIM-SM packets sent by Router B in 1s before the speed is configured. The information should be displayed as follows:</p>
	<pre>Qtech #show ip pim sparse mode track PIM packet counters track Elapsed time since counters cleared: 04d01h04ms received sent Valid PIM packets: 18765 29789 Hello: 11154 17852 Join Prune: 0 3236 Register: 0 3214 Register Stop: 3195 0 Assert: 0 0 BSM: 0 5487 C RP ADV: 4416 0 PIMDM Graft: 0 PIMDM Graft Ack: 0 PIMDM State Refresh: 0 Unknown PIM Type: 0 Errors: Malformed packets: 0 Bad checksums: 0 Send errors: 0 Packets received with unknown PIM version: 0 Qtech#</pre>
	<p>Display the number of PIM-SM packets sent by Router B after the speed is configured. The information should be displayed as follows:</p>
	<pre>Qtech#show ip pim sparse mode track PIM packet counters track Elapsed time since counters cleared: 04d01h06m</pre>

	received	sent
Valid PIM packets:	18777	29808
Hello:	11159	17862
Join Prune:	0	3239
Register:	0	3215
Register Stop:	3196	0
Assert:	0	0
BSM:	0	5489
C RP ADV:	4419	0
PIMDM Graft:	0	
PIMDM Graft Ack:	0	
PIMDM State Refresh:	0	
Unknown PIM Type:	0	
Errors:		
Malformed packets:		0
Bad checksums:		0
Send errors:		0
Packets received with unknown PIM version: 0		
Qtech#		

❖ Configuring the Checksum of the Register Packet Length

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ Calculate the checksum of the entire register packet length. ➤ Run show running-config to check whether the preceding configurations take effect.
	Qtech(config)#ip pim register checksum wholepkt
Verification	Display the configurations on Router A, which should be as follows:
	<pre>Qtech#show running config ! ip pim register checksum wholepkt ip pim rp candidate Loopback 0</pre>

```
!
. . . .
```

❖ Enabling an RP to Decapsulate a Register Packet and Forward the Multicast Packet to Interfaces

<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ Enable Router A to forward a register packet. ➤ Run show running-config to check whether the preceding configurations take effect.
	<pre>Qtech(config)#ip pim register decapsulate forward</pre>
<p>Verification</p>	<p>Display the configurations on Router A, which should be as follows:</p>
	<pre>Qtech#show running config ! ! ip pim register decapsulate forward ip pim register checksum wholepkt ip pim rp candidate Loopback 0 ! ! !</pre>

❖ Configuring the Source IP Address of a Register Packet

<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ Configure the source address of Loop 2 as 192.168.2.2. ➤ Configure source address interface for the register packet of Router B as Loop 2. ➤ Run show running-config to check whether the preceding configurations take effect.
<p>Verification</p>	<p>Display the configurations on Router B, which should be as follows:</p>
	<pre>Qtech#show running config ! ! ! ip pim register source Loopback 1</pre>

```
ip pim bsr candidate Loopback 0
!
!
!
!
```

❖ Configuring the Suppression Time of a Register Packet and the Inspection Time of a Null Register Packet

<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ Configure the suppression time of a register packet on Router B to 20s. ➤ Configure the inspection time of a null register packet on Router B to 2s. ➤ Run show ip pim sparse-mode track to display number of register packets.
	<pre>Qtech(config)#ip pim register suppression 20 Qtech(config)#ip pim probe interval 2</pre>
<p>Verification</p>	<p>Display the number of register packets on Router B. The information should be displayed as follows:</p>
	<pre>Qtech#show ip pim sparse mode track PIM packet counters track Elapsed time since counters cleared: 04d23h15m received sent Valid PIM packets: 23788 43249 Hello: 13817 23178 Join Prune: 0 4568 Register: 0 8684 Register Stop: 4223 0 Assert: 0 0 BSM: 0 6819 C RP ADV: 5748 0 PIMDM Graft: 0 PIMDM Graft Ack: 0 PIMDM State Refresh: 0 Unknown PIM Type: 0</pre>

	<pre> Errors: Malformed packets: 0 Bad checksums: 0 Send errors: 0 Packets received with unknown PIM version: 0 Qtech# Qtech# </pre>
	<p>In 18s, display the number of register packets on Router B. The information should be displayed as follows:</p>
	<pre> Qtech#show ip pim sparse mode track PIM packet counters track Elapsed time since counters cleared: 04d23h17m received sent Valid PIM packets: 23798 43263 Hello: 13820 23184 Join Prune: 0 4569 Register: 0 8685 Register Stop: 4224 0 Assert: 0 0 BSM: 0 6820 C RP ADV: 5749 0 PIMDM Graft: 0 PIMDM Graft Ack: 0 PIMDM State Refresh: 0 Unknown PIM Type: 0 Errors: Malformed packets: 0 Bad checksums: 0 Send errors: 0 Packets received with unknown PIM version: 0 Qtech# </pre>

❖ Configuring an RP to Receive Register Packets and the (S, G) Lifetime

<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ Configure Router A to receive register packets and the (S, G) lifetime is 60s. ➤ Run show ip pim sparse-mode mroute to display number of register packets.
	<pre>Qtech(config)#ip pim rp register kat 60</pre>
<p>Verification</p>	<p>After the lifetime is configured, check that the (S, G) lifetime on Router A does not exceed 60s.</p>
	<pre>Qtech(config)#show ip pim sparse mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 0 (192.168.1.100, 233.3.3.3) RPF nbr: 192.168.36.90 RPF idx: VLAN 1 SPT bit: 0 Upstream State: NOT JOINED kat expires in 49 seconds 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 Joined 0 Asserted 0 Outgoing</pre>

```
0 . . . . .
. . . . .

(192.168.1.100, 233.3.3.3, rpt)
RP: 192.168.8.8
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: RPT NOT JOINED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31
Local
0 . . . . .
. . . . .
Pruned
0 . . . . .
. . . . .
Outgoing
0 . . . . .
. . . . .

(*, 239.255.255.250)
RP: 192.168.8.8
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31
Local
0 . . . . .
. . . . .
Joined
0 .
j . . . . .
. . . . .
Asserted
```

```

0 . . . . .
. . . . .
FCR:

Qtech(config)#
Qtech(config)#show ip pi

```

Common Errors

- Basic PIM-SM functions are not configured or the configuration is not successful.
- The (S, G) of register packets is not configured on a C-RP or static RP, or the configuration is not successful.
- The ACL for limiting the (S, G) of register packets is not configured or the range of (S, G) in this ACL is not correctly configured.
- The range of (S, G) of register packets on each C-RP or static RP is not the same.

6.4.5 Configuring the Interval for Sending a Join/Prune Packet

Configuration Effect

- Change the interval for sending a Join/Prune packet to form an RPT or SPT.

Notes

- Basic PIM-SM functions must be configured.

Configuration Steps

- Configure the interval for sending a Join/Prune packet.

Verification

On Router B, configure the interval for sending a Join/Prune packet as 120s. Run **show ip pim sparse-mode mroute** to display the lifetime of the entry.

Related Commands

- ❖ Configuring the Interval for Sending a Join/Prune Packet

Command	ip pim jp-timer <i>seconds</i>
Parameter	<i>Seconds</i> : Indicates the interval for sending a Join/Prune packet.
Description	The unit is second. The value ranges from 1 to 65,535 (60 by default).
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

❖ Configuring the Interval for Sending a Join/Prune Packet

<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ Configure the interval for sending a Join/Prune packet.
	<pre>Qtech(config)#ip pim jp timer 120</pre>
<p>Verification</p>	<p>Run show ip pim sparse-mode mroute to display the maximum timeout time of a Join/Prune packet.</p>
	<pre>Qtech(config)#show ip pim sparse mode mroute IP Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 1 (192.168.1.100, 233.3.3.3) RPF nbr: 0.0.0.0 RPF idx: None SPT bit: 1 Upstream State: JOINED jt_timer expires in 96 seconds kat expires in 92 seconds 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 1 Joined 0 1</pre>

```
Asserted
0 . . . . .
. . . . .
1 . . . . .
. . . . .

Outgoing
0 . . . . .
. . . . .
1 . .
0 . . . . .
. . . . .
.

(192.168.1.100, 233.3.3.3, rpt)
RP: 192.168.8.8
RPF nbr: 192.168.36.89
RPF idx: GigabitEthernet 0/1
Upstream State: RPT NOT JOINED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31

Local
0 . . . . .
. . . . .
1 . . . . .
. . . . .

Pruned
0 . . . . .
. . . . .
1 . . . . .
. . . . .

Outgoing
0 . . . . .
. . . . .
1 . . . . .
. . . . .
```

```
(*, 239.255.255.250)
RP: 192.168.8.8
RPF nbr: 192.168.36.89
RPF idx: GigabitEthernet 0/1
Upstream State: JOINED
jt_timer expires in 119 seconds
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31
Local
0 . . . . .
i . . . . .
. . . . .
1 . . . . .
. . . . .
Joined
0 . . . . .
. . . . .
1 . . . . .
. . . . .
Asserted
0 . . . . .
. . . . .
1 . . . . .
. . . . .
FCR:
VSU(config)#
```

Common Errors

- Basic PIM-SM functions are not configured or the configuration is not successful.

6.4.6 Configuring the Router of Last Hop to Switch from an RPT to SPT

Configuration Effect

- Switch from an RPT to SPT

Notes

- Basic PIM-SM functions must be configured.

Configuration Steps

- Configure the router of last hop to switch from an RPT to SPT.

Verification

Configure basic PIM-SM functions first. Configure the source DR to send the data traffic (*, 233.3.3.3), and the receiving end to join group 233.3.3.3 forcibly to form an RPT. Configure the receiver DR to switch from the RPT to SPT forcibly. Run **show running-config** to display the result.

Related Commands

- ❖ Enabling SPT switchover

Command	<code>ip pim spt-threshold [group-list access-list]</code>
Parameter Description	<p>group-list access-list: Specifies the range of multicast group addresses allowed for SPT switchover using an ACL.</p> <p>access-list: The supported value ranges from 1 to 99 or 1,300 to 1,999. Naming an ACL is also supported.</p>
Command Mode	Global configuration mode
Usage Guide	If group-list access-list is not specified, all groups are allowed to perform SPT switchover.

Configuration Example

- ❖ Configuring the Router of Last Hop to Switch from an RPT to SPT

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic PIM-SM functions. (Omitted) ➤ Configure the source DR to send the data traffic of group 233.3.3.3. ➤ Configure the receiver DR to receive the data traffic of group 233.3.3.3. ➤ Configure the receiver DR of last hop to switch from an RPT to SPT.
	<pre>Qtech(config)#ip pim spt threshold</pre>
Verification	Run show running-config to display the configuration.
	<pre>! ! ip pim jp timer 120 ip pim spt threshold ip pim rp candidate Loopback 0 ! ! !</pre>

6.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears multicast routing entries.	clear ip mroute { * <i>group-address</i> [<i>source-address</i>] }
Clears the counters of multicast routes.	clear ip mroute statistics { * <i>group-address</i> [<i>source-address</i>] }
Clears the information about dynamic RPs.	clear ip pim sparse-mode bsr rp-set *
Clears the counters of PIM-SM packets.	clear ip pim sparse-mode track

Displaying

Description	Command
Displays the details of BSR information.	show ip pim sparse-mode bsr-router
Displays the PIM-SM information of an interface.	show ip pim sparse-mode interface [<i>interface-type interface-number</i>] [detail]
Displays the local IGMP information about a PIM-SM interface.	show ip pim sparse-mode local-members [<i>interface-type interface-number</i>]
Displays the information about a PIM-SM multicast routing entry, and displays the RPF vector of a PIM-SM entry using proxy .	show ip pim sparse-mode mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]] [proxy]
Displays the information about PIM-SM neighbors.	show ip pim sparse-mode neighbor [detail]
Displays the information about the next hop of PIM-SM obtained from the NSM.	show ip pim sparse-mode nexthop
Displays the information about the RP corresponding the multicast group address <i>group-address</i> .	show ip pim sparse-mode rp-hash <i>group-address</i>
Displays the information about all the RPs and the groups they serve.	show ip pim sparse-mode rp mapping
Displays the number of PIM-SM packets sent and received since the statistic start time.	show ip pim sparse-mode track

7. CONFIGURING PIM-SMV6

7.1 Overview

Protocol Independent Multicast (PIM) is a multicast routing protocol.

PIM does not rely on a specific unicast routing protocol. It uses the unicast routing table established by any unicast routing protocol to complete the reverse path forwarding (RPF) check and establish multicast routes. PIM does not need to transmit and receive multicast route updates. Therefore, the overhead of PIM is much lower than that of other multicast routing protocols.

PIM defines two modes: dense mode and sparse mode. Protocol Independent Multicast Sparse Mode (PIM-SM) is applicable to various network environments.

- PIM-SM running on IPv6 is called PIM-SMv6.

Protocols and Standards

- RFC4601: Protocol Independent Multicast -Sparse Mode (PIM-SM)
- RFC5059: Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)
- RFC3962: Protocol Independent Multicast - Dense Mode protocol
- RFC4607: Source-Specific Multicast for IP

7.2 Applications

Application	Description
ASM Implementation by Using PIM-SMv6	A receiver receives packets from any multicast source.
SSM Implementation by Using PIM-SMv6	A receiver selects a multicast source.
Application Example of an Embedded RP	An embedded RP address is configured within the IPv6 multicast group address.
PIM-SMv6 Application in a Hot Backup Environment	The multicast PIM-SMv6 protocol runs in a hot backup environment.

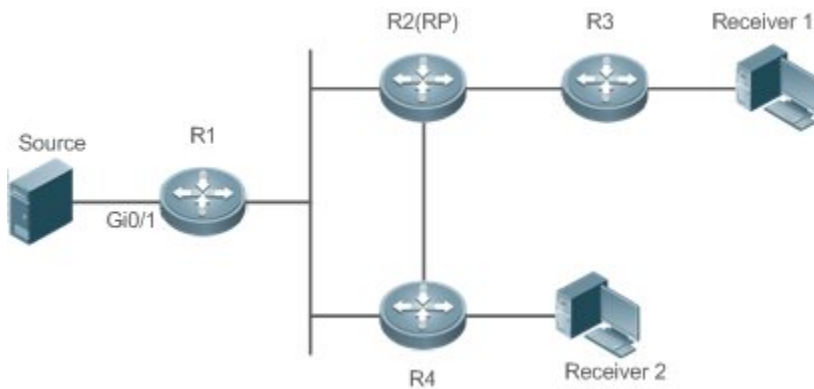
7.2.1 ASM Implementation by Using PIM-SMv6

Scenario

The multicast service is provided only in one domain.

As shown in the following figure, receivers receive packets from any multicast source.

Figure 7-1



Remark	R1 is directly connected to the multicast source.
s	R2 is configured as a rendezvous point (RP).
	R3 is directly connected to Receiver A.
	R4 is directly connected to Receiver B.

Deployment

- Run the Open Shortest Path First for IPv6 (OSPFv6) protocol in the domain to implement unicast routing.
- Run the PIM-SMv6 protocol in the domain to implement multicast routing.
- Run the Internet Group Management Protocol version 6 (IGMPv6) protocol in a user host network segment to implement group member management.

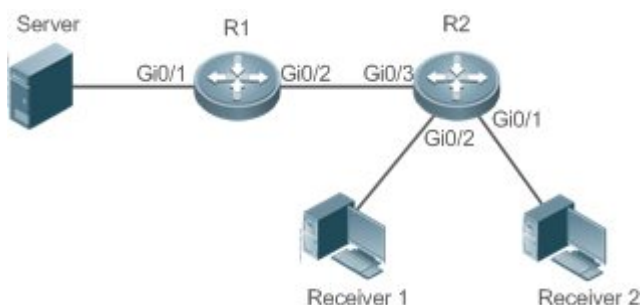
7.2.2 SSM Implementation by Using PIM-SMv6

Scenario

The multicast service is provided only in one domain.

As shown in the following figure, receivers receive packets from a specific multicast source.

Figure 7-2



Remark	R1 is directly connected to the multicast source.
s	R2 is configured as an RP.
	R2 is directly connected to Receiver A.
	R2 is directly connected to Receiver B.

Deployment

- Run the OSPFv6 protocol in the domain to implement unicast routing.
- Run the PIM-SMv6 protocol in the domain to implement multicast routing.
- Enable the source-specific multicast (SSM) function of the PIM-SMv6 protocol to implement the SSM function.
- Run the Internet Group Management Protocol version 3 (IGMPv3) in a user host network segment to implement group member management.

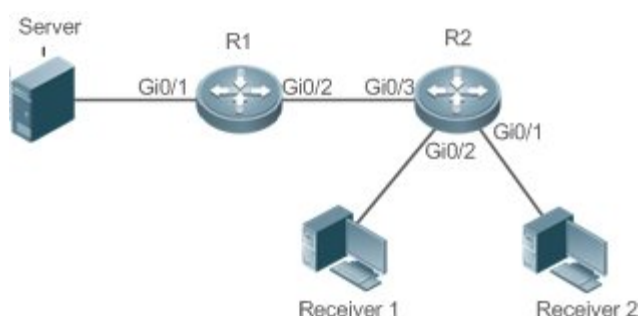
7.2.3 Application Example of an Embedded RP

Scenario

The multicast service is provided only in one domain.

As shown in the following figure, an RP address is configured for R2 to make the router become an embedded RP.

Figure 7-3



Remarks	<p>R1 is directly connected to the multicast source.</p> <p>R2 is configured as an RP.</p> <p>R2 is directly connected to Receiver A.</p> <p>R2 is directly connected to Receiver B.</p> <p>R2 is configured as an embedded RP.</p>
----------------	---

Deployment

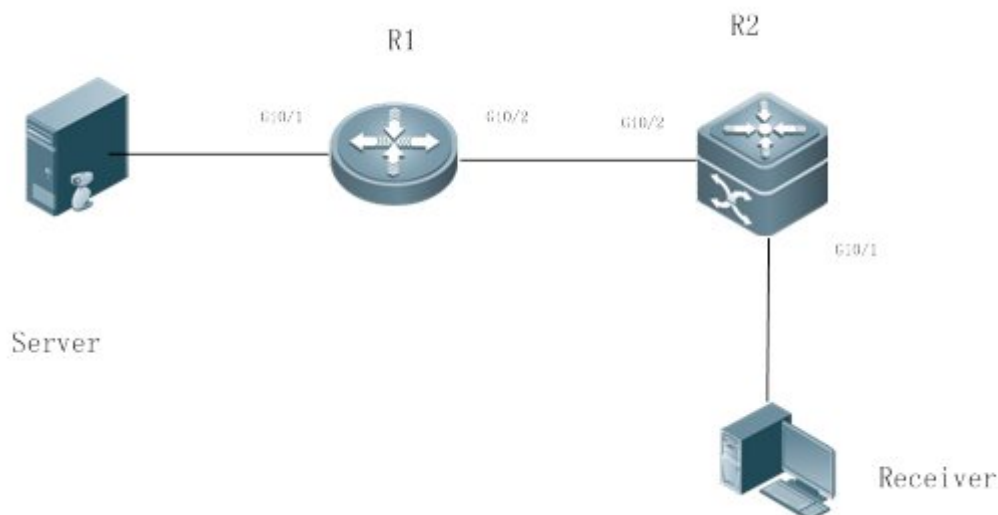
- Run the OSPFv6 protocol in the domain to implement unicast routing.
- Run the PIM-SMv6 protocol in the domain to implement multicast routing.
- Enable the SSM function of the PIM-SMv6 protocol to implement the SSM function.
- Run the IGMPv3 protocol in a user host network segment to implement group member management.
- Configure the RP address and embedded RP on R2.

7.2.4 PIM-SMv6 Application in a Hot Backup Environment

Scenario

In a hot backup environment, run PIM-SMv6. A device performs hot backup switching to ensure that traffic is not interrupted.

Figure 7-4



Remarks	<p>R1 is connected to the video server, R2 is directly connected to the receiver, and R2 runs in hot backup mode.</p> <p>A Layer-3 multicast protocol runs on R1 and R2.</p>
----------------	--

Deployment

- Run OSPF on R1 and R2 to implement unicast routing.
- Run PIM-SMv6 on R1 and R2 to implement multicast routing.
- Make R2 run in two-node cluster hot backup mode.

Remarks	<p>R2 may perform hot backup switching in the hot backup environment. In this case, the query interval of PIM Hello packets (the default value is 30 seconds) needs to be adjusted on R2 because the keepalive timer of the neighbor in PIM Hello packets of R1 may have expired (the default value is 3.5 times the query interval, that is, 105 seconds). The multicast function relies on the unicast function currently, and the multicast function starts convergence after the unicast function convergence is complete. For example, the default graceful restart (GR) convergence time of the unicast function is 120 seconds. It is recommended that the query interval of PIM Hello packets be set to 60 seconds. The keepalive time of the neighbor in PIM Hello packets is 210 seconds. In this scenario, the query interval of PIM Hello packets need to be set with a reference to the GR convergence time of the unicast function and the value of 3.5 times the query interval of PIM Hello packets must be larger than the GR convergence time of the unicast function. In addition, if the convergence time of the unicast function is long, the transmission interval of PIM</p>
----------------	---

Join/Prune packets also need to be adjusted, because the keepalive time of PIM Join/Prune packets is 3.5 times the transmission interval of PIM Join/Prune packets. The default keepalive time of PIM Join/Prune packets is 210 seconds. If R2 is configured as a dynamic RP, the interval for a candidate RP (C-RP) to transmit C-RP notifications also needs to be adjusted. The default transmission interval is 60 seconds and the keepalive time is 2.5 times the transmission interval of C-RP notifications. For example, if the convergence time of the unicast function is longer than 150 seconds, the transmission interval of C-RP notifications needs to be adjusted. In a hot backup environment, it is recommended that the query interval of PIM Hello packets be larger than the default value (30 seconds). Otherwise, the keepalive timer of the neighbor in PIM Hello packets of the peer end times out during hot backup switching.

7.3 Features

Basic Concepts

❖ PIM Router and PIM Interface

Routers where the PIM protocol is enabled are called PIM routers. Interfaces where the PIM protocol is enabled are called PIM interfaces.

Multicast packets are forwarded by PIM routers. The PIM interfaces for receiving multicast packets are called upstream interfaces, and the PIM interfaces for transmitting multicast packets are called downstream interfaces.

Network segments where upstream interfaces are located are called upstream network segments. Network segments where downstream interfaces are located are called downstream network segments.

❖ PIM Network and PIM Domain

PIM routers are connected through PIM interfaces and form a PIM network.

On some PIM interfaces, borders are set to divide a large PIM network into multiple PIM domains. The borders may reject specific multicast packets or limit transmission of PIM messages.

❖ Multicast Distribution Tree, DR, RP

Multicast packets are transmitted from one point to multiple points. The forwarding path presents a tree structure. This forwarding path is called a multicast distribution tree (MDT). MDTs are classified into two types:

- Rendezvous point tree (RPT): Uses the rendezvous point (RP) as the root and designated routers (DRs) connected to group members as leaves.
- Shortest path tree (SPT): Use the DR connected to a multicast source as the root and the RPs or DRs connected to group members as leaves.

DRs and RPs are function roles of PIM routers.

- RPs collect information about multicast sources and group members in the network.

- The DR connected to a multicast source reports multicast source information to the RP and the DRs connected to group members report the group member information to the RP.
- ❖ (*,G), (S,G)
- (*,G): Indicates the packets transmitted from any source to Group G, routing entries corresponding to the packets, and forwarding path (RPT) corresponding to the packets.
- (S,G): Indicates the packets transmitted from Source S to Group G, routing entries corresponding to the packets, and forwarding path (SPT) corresponding to the packets.
- ❖ ASM, SSM

PIM-SM supports two multicast service models: any-source multicast (ASM) and source-specific multicast (SSM), which are applicable to different multicast address segments.

- ASM: In the ASM model, a user host cannot select a multicast source. The user host joins a multicast group and receives all packets sent from all sources to the multicast group.
 - SSM: In the SSM model, a user host can select a multicast source. The user host specifies the source address when joining a multicast group, and then receives packets only from the specified source to the multicast group.
-
- SSM model requirement: Other network services must be used to enable a user host to know the position of a multicast source in advance so that the user host selects the multicast source.

Overview

Feature	Description
Establishment of PIM Neighbor Relationships	Neighbor relationships are established between PIM routers to form a PIM network.
DR Election	In the shared network segment connected to group members, DR election is conducted among PIM neighbors to elect the DR connected to group members. In the shared network segment connected to a multicast source, DR election is conducted among PIM neighbors to elect the DR connected to the multicast source.
RP Mechanism	In a PIM network, the RP is statically configured or dynamically elected so that each PIM router knows the position of the RP.
Registration Information About a Multicast Source	When a multicast source arises in a network, the DR connected to the multicast source transmits the Register packet to the RP so that the RP obtains information about the multicast source and multicast packets.
RPT Establishment	When a group member arises in a network, the DR connected to the group member transmits the Join packet in the RP direction to establish an RPT. If there is a multicast source in the network, the multicast packet transmitted to the RP can reach the group member along the RPT.
SPT Establishment	When a data packet reaches the DR connected to a group member, the DR connected to the group member transmits the Join packet in the multicast source direction to establish an SPT. Then, multicast packets are forwarded along the SPT.

[ASM and SSM Models](#)

PIM routers provide multicast services of the ASM model and SSM model. The SSM model is used for groups within the SSM address range, and the ASM model is used for other groups.

7.3.1 Establishment of PIM Neighbor Relationships

Neighbor relationships are established between PIM routers to form a PIM network. Neighbor relationships must be established between PIM routers before other PIM control messages are exchanged or multicast packets are forwarded.

Working Principle

A Hello message is sent by a PIM interface. For the multicast packet for encapsulating the Hello message, the destination address is ff02::d (indicating all PIM routers in the same network segment), the source address is the IP address of the PIM interface, and the time to live (TTL) value is 1.

Hello messages are used to discover neighbors, negotiate about protocol parameters, and maintain neighbor relationships.

❖ Discovering PIM Neighbors

PIM routers in the same network segment receive multicast packets with the destination address of ff02::d. In this way, the PIM routers obtain neighbor information and establish neighbor relationships.

When a PIM interface is enabled or detects a new neighbor, the Triggered-Hello-Delay message is used to generate a random time period. Within the time period, the interface sends Hello packets.

❖ Negotiating About Protocol Parameters

A Hello message contains multiple protocol parameters, which are described as follows:

- DR_Priority: Indicates the priority of each router interface for DR election. A higher priority means a higher possibility of being elected as the DR.
- Holdtime: Indicates the timeout time in which a neighbor is held in the reachable state.
- LAN_Delay: Indicates the delay for transmitting a Prune message in a shared network segment.
- Override-Interval: Indicates the prune override time carried in a Hello message.

When a PIM router receives a Prune message from an upstream interface, it indicates that other downstream interfaces exist in the shared network segment. If the PIM router still needs to receive multicast data, it must send a Prune Override message to the upstream interface within the time of **Override-Interval**.

$LAN_Delay + Override-Interval = PPT$ (Prune-Pending Timer). After a PIM router receives a Prune message from a downstream interface, it does not immediately perform pruning but waits for PPT timeout. After the PPT times out, the PIM router performs pruning. Within the time of PPT, if the PIM router receives a Prune Override message from the downstream interface, it cancels pruning.

❖ Maintaining Neighbor Relationships

A Hello message is sent periodically between PIM routers. If a Hello packet is not received from a PIM neighbor within Holdtime, the neighbor is considered unreachable and is deleted from the neighbor list. Any changes in PIM neighbors will cause multicast topology changes in the network. If an upstream neighbor or a downstream neighbor in an MDT is unreachable, multicast routing re-convergence is performed again and the MDT is migrated.

Related Configuration

❖ Enabling the PIM-SMv6 Function on an Interface

By default, the PIM-SMv6 function is disabled on an interface.

Run the **ipv6 pim sparse-mode** command to enable or disable the PIM-SMv6 function on an interface.

The PIM-SMv6 function must be enabled on an interface so that the interface participates in the operation of PIM protocols. If the PIM-SMv6 function is disabled on an interface that functions as a DR, static RP, candidate - rendezvous point (C-RP), or candidate – bootstrap router (C-BSR), the corresponding protocol role does not take effect.

❖ Adjusting the Transmission Interval of Hello Messages on an Interface

By default, Hello messages are transmitted at an interval of 30 seconds.

Run the **ipv6 pim query-interval seconds** command to adjust the transmission interval of Hello messages on an interface. The value ranges from 1 to 65,535.

A larger value of *interval-seconds* means a larger transmission interval of Hello messages and a smaller value of *interval-seconds* means a smaller transmission interval of Hello messages.

7.3.2 DR Election

In the shared network segment connected to group members, DR election is conducted among PIM neighbors to elect the DR connected to the group members.

In the shared network segment connected to a multicast source, DR election is conducted among PIM neighbors to elect the DR connected to the multicast source.

The DR transmits the Join/Prune message in the MDT root node direction for the directly connected group members, or transmits data of the directly connected multicast source to the MDT.

Working Principle

The neighbor IP address and DR priority are obtained from Hello packets of neighbors during establishment of PIM neighbor relationships, so as to elect the DR.

The key of DR election is the DR priorities and IP addresses of interfaces.

❖ Interface DR Priority

A higher interface DR priority means a higher probability that a PIM router is successfully elected as the DR during the DR election.

❖ Interface IP Address

If interfaces of PIM routers share the same DR priority during DR election, IP addresses of neighbors are compared. A larger IP address means a higher probability that a PIM router is successfully elected as the DR.

Related Configuration

❖ Setting IP Addresses of Interfaces

By default, no IP addresses are configured for interfaces.

Run the **ipv6 address** command to set an IP address for an interface.

When PIM routers share the same DR priority, the PIM router with a larger IP address is elected as the DR.

❖ Enabling the PIM-SMv6 Function on an Interface

By default, the PIM-SMv6 function is disabled on an interface.

Run the **ipv6 pim sparse-mode** command to enable or disable the PIM-SMv6 function on an interface.

The PIM-SMv6 function must be enabled on an interface so that the interface participates in the operation of PIM protocols. If the PIM-SMv6 function is disabled on an interface that functions as a DR, static RP, C-RP, or C-BSR, the corresponding protocol role does not take effect.

❖ Adjusting the DR Priority of an Interface

By default, the DR priority is 1.

Run the **ipv6 pim dr-priority *priority-value*** command to adjust the DR priority of an interface. The priority value ranges from 0 to 4,294,967,294.

The DR priority of an interface is used to elect the DR in the directly connected network segment of the interface. A larger priority value means a higher probability that a PIM router is elected as the DR.

7.3.3 BSR Mechanism

In a PIM network, the bootstrap router (BSR) periodically generates bootstrap messages (BSMs) including information about a series of C-RPs and relevant group addresses. BSMs are transmitted hop by hop in the entire domain. PIM routers throughout the network receive BSMs and record information about C-RPs and the relevant group addresses.

Working Principle

One or more C-BSRs are configured in the PIM-SMv6 domain and the BSR is elected from the candidate BSRs according to certain rules.

Related Configuration

❖ Configuring a C-BSR

By default, no C-BSR is configured.

Run the **ipv6 pim bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority-value*]] command to configure or cancel a C-BSR.

C-BSRs elect the globally unique BSR in the PIM-SM domain by means of BSM learning and election. The BSR transmits BSMs.

❖ Configuring the BSR Border

By default, no BSR border is configured.

Run the **ipv6 pim bsr-border** command to configure or cancel the BSR border.

After this command is configured for an interface, the interface immediately discards the received BSMs and does not forward BSMs, thereby preventing BSM flooding. No BSR border is configured if this command is not configured.

❖ Defining the Valid BSR Range

By default, the BSMs of BSRs are not filtered.

Run the **ipv6 pim accept-bsr list** *ipv6_access-list* command to define or cancel the BSR range.

After this command is configured, the valid BSR range is defined. If this command is not configured, the device with the PIM-SMv6 function enabled will receive all BSMs.

❖ Configuring a C-BSR to Restrict the Address Range of Valid C-RPs and the Range of Multicast Groups Served by the C-RPs

A C-BSR receives notifications from all C-RPs.

Run the **ipv6 pim accept-crp list** *ipv6_access-list* command to configure whether to filter notifications from C-RPs.

After this command is configured, the C-BSR restricts the address range of valid C-RPs and the range of multicast groups served by the C-RPs. If this command is not configured, the C-BSR receives notifications from all C-RPs.

❖ Configuring a C-BSR to Receive C-RP-ADV Packets with prefix-count of 0

By default, a C-BSR does not receive C-RP-ADV packets with prefix-count of 0.

Run the **ipv6 pim accept-crp-with-null-group** command to configure whether to receive C-RP-ADV packets with prefix-count of 0.

After this command is configured, the C-BSR can receive C-RP-ADV packets with prefix-count of 0. If this command is not configured, the C-BSR does not process C-RP-ADV packets with prefix-count of 0.

7.3.4 RP Mechanism

In a PIM network, the RP is statically configured or dynamically elected so that each PIM router knows the position of the RP. The RP serves as the root of the RPT. The RPT establishment and the forwarding of RPT data streams must use the RP as the forwarding point.

Working Principle

All PIM routers in a PIM domain must be able to be mapped to the same RP through a specific multicast group address. RPs are classified into static RPs and dynamic RPs in a PIM network.

❖ Static RP

In static RP configuration, the RP address is directly configured on each PIM router so that all PIM routers in the PIM network know the RP address.

❖ Dynamic RP

C-RPs are also configured in the PIM-SMv6 domain. These C-RPs transmit data packets that contain their addresses and information about multicast groups served by them to the BSR in unicast mode. The BSR periodically generates BSMs that contain information about a series of C-RPs and their group addresses. BSMs are transmitted hop by hop in the entire domain. Devices receive and store these BSMs. The DR at the receive end uses a hash algorithm to map a group address to the C-RP that can serve the group. Then, the RP corresponding to the group address can be determined.

Related Configuration

❖ Setting a Static RP Address

By default, no RP address is configured.

Run the **ipv6 pim rp-address** *ipv6_rp-address* [*ipv6_access-list*] command to configure or cancel a static RP address for a PIM router.

An RP must be configured so as to implement ASM in a PIM-SMv6 network. You can configure a static RP or dynamic RP.

If a static RP is configured in a PIM-SMv6 network, the static RP configuration on all devices in the PIM-SMv6 domain must be consistent to prevent multicast route ambiguity in the PIM-SMv6 domain.

❖ Configuring a C-RP Address

By default, no C-RP address is configured.

Run the **ipv6 pim rp-candidate** *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *ipv6_access-list*] command to configure or cancel a PIM router as a C-RP.

C-RPs periodically transmit C-RP notifications to the BSR. Information contained in these C-RP notifications is dispersed to all PIM-SMv6 devices in the domain, thereby ensuring the uniqueness of RP mapping.

❖ Ignoring the RP Priority in RP Setting

By default, a C-RP with a higher priority is selected preferentially.

Run the **ipv6 pim ignore-rp-set-priority** command to specify or ignore the RP priority when selecting the RP for a group.

When one RP needs to be selected for a multicast address and multiple RPs can serve this multicast address, use this command if the RP priority needs to be ignored during the RP comparison. If this command is not configured, the RP priority will be considered during the RP comparison.

❖ Configuring the Static RP First

By default, a dynamic C-RP is adopted preferentially.

Run the **ipv6 pim static-rp-preferred** command to select the static RP first during RP selection.

After this command is configured, the static RP is adopted first. If this command is not configured, a C-RP is adopted first.

❖ Configuring the Embedded RP Function

By default, the embedded RP function is enabled for all IPv6 multicast group addresses where the RP address is embedded.

Run the **ipv6 pim rp embedded [group-list *ipv6_acl_name*]** command to enable the embedded RP function.

The embedded RP function is the peculiar RP discovery mechanism of IPv6 PIM. This mechanism uses the IPv6 multicast address where the RP address is embedded, to enable a multicast device to directly extract the RP address from the multicast address. By default, the embedded RP function is enabled for all IPv6 multicast group addresses where the RP address is embedded.

7.3.5 Registration Information About a Multicast Source

When a multicast source arises in a network, the DR connected to the multicast source transmits the Register packet to the RP so that the RP obtains information about the multicast source and multicast packets.

Working Principle

The DR at the data source end receives a multicast data packet from the directly connected host, and encapsulates the multicast data into a Register message. Then, it transmits the Register message to the RP in unicast mode. The RP generates the (S,G) entry.

If the forwarding entry contains an outgoing interface on the RP, the RP forwards the encapsulated data packet to the outgoing interface.

If the RP does not have the forwarding entry of the current group, it starts the (S,G) entry start timer. After the timer expires, the RP transmits the Register-Stop message to the DR and deletes the entry.

After the DR at the data source end receives the Register-Stop message, the DR transmits the probing packet before the Register-Stop message timer expires.

If the DR does not receive the Register-Stop message, after the timer expires, the DR at the data source end encapsulates the multicast data into the Register message and transmits it to the RP in unicast mode.

If the DR receives the Register-Stop message, it re-starts the delay and re-transmits the probing packet before the delay expires.

Related Configuration

❖ Configuring Reachability Detection of RP Register Packets

By default, the RP reachability is not detected.

Run the **ipv6 pim register-rp-reachability** command to set or cancel the RP reachability detection.

If the RP reachability needs to be detected for the Register packet transmitted from the DR to the RP, you can configure this command. After this command is configured, the RP reachability is detected before the DR transmits the Register packet to the RP. That is, the DR queries the unicast routing table and static multicast routing table to check whether a route reachable to the RP exists. If no, the DR does not transmit the Register packet.

❖ Configuring the RP to Filter Register Packets

By default, the RP allows every received Register packet.

Run the **ipv6 pim accept-register { list ipv6_access-list [route-map map-name] | route-map map-name [list ipv6_access-list] }** command to enable or disable the RP to filter received Register packets.

To filter received Register packets on the RP, configure this command. If this command is not configured, the RP allows every received Register packet. If this command is configured, only Register packets whose source addresses and group addresses are allowed by the ACL are processed. Otherwise, the Register packets are filtered out.

❖ Configuring the Transmission Rate Limit for Register Packets

By default, the transmission rate of Register packets is not limited.

Run the **ipv6 pim register-rate-limit rate** command to configure whether to limit the transmission rate of Register packets.

If **no** is set in this command, the transmission rate is not limited. This command is used to configure the transmission rate of Register packets from the (S,G) multicast group address rather than the transmission rate of Register packets of the entire system.

❖ Configuring the Checksum Calculation of a Register Packet Based on the Entire Register Packet

By default, the checksum in a Register packet is calculated in default mode specified in the protocol.

Run the **ipv6 pim register-checksum-wholepkt [group-list *ipv6_access-list*]** command to set the packet length for checksum calculation.

If the entire PIM protocol packet including the encapsulated multicast data packet is used for checksum calculation of a Register packet, use this command. If this command is not configured, the checksum in a Register packet is calculated in default mode specified in the protocol.

❖ Configuring the Source Address of Register Packets

By default, the source address of Register packets uses the address of the DR interface connected to a multicast source.

Run the **ipv6 pim register-source { *ipv6_local_address* | *interface-type interface-number* }** command to configure the source address of Register packets.

To configure the source address of Register packets transmitted from the DR, use this command. If this command is not configured or **no** is set in this command, the source address of Register packets uses the address of the DR interface connected to a multicast source. If the address parameter of this command is used, the configured address must be a reachable unicast route. If the interface parameter of this command is used, this interface may be a loopback interface or an interface of other types and the interface address must be an advertised unicast route.

❖ Configuring the Suppression Time of Register Packets

The default suppression time of Register packets is 60 seconds.

Run the **ipv6 pim register-suppression *seconds*** command to configure the suppression time.

If this command is used to configure the suppression time of Register packets, configuring the value on the DR will change the suppression time of Register packets on the DR. If the **ipv6 pim rp-register-kat *seconds*** command is not configured, defining the value on the RP will change the keepalive time on the RP.

❖ Configuring the Probing Time of NULL Register Packets

The default probing time is 5 seconds.

Run the **ipv6 pim probe-interval *interval-seconds*** command to set the probing time.

The source DR transmits the NULL-Register packet to the RP within a certain interval prior to the timeout of the suppression time of the Register packet. This interval is the probing time. The default probing time is 5 seconds.

❖ Configuring the Time Value of the RP KAT Timer

By default, the KAT default value is used. KAT default value = Registration suppression time x 3 + Registration detection time.

Run the **ipv6 pim rp-register-kat *seconds*** command to set time of the KAT timer.

To configure the keepalive time of Register packets from the (S,G) multicast group address on the RP, use this command.

7.3.6 RPT Establishment

When a group member arises in a network, the DR connected to the group member transmits the Join packet in the RP direction to establish an RPT. If there is a multicast source in the network, the multicast packet transmitted to the RP can reach the group member along the RPT.

Working Principle

The RPT establishment process is as follows:

- 8) The DR at the receive end receives an MLD (*,G)Include report packet from a receiver.
- 9) If the DR at the receive end is not the RP of Group G, the DR at the receive end transmits one (*,G)join packet in the RP direction. The upstream device that receives the (*,G)join packet transmits the (*,G)join packet in the RP direction. The (*,G)join packet is transmitted hop by hop till the RP of Group G receives the (*,G)join packet, indicating that the DR at the receive end joins the RPT.
- 10) When the data source host transmits multicast data to a group, the source data is encapsulated into the Register message and is transmitted to the RP in unicast mode by the DR at the data source end. The RP decapsulates the Register message, retrieves the data packet, and then forwards it to each group member along the RPT.
- 11) The RP transmits the (S,G)join packet to the DR at the data source end to join the SPT of this data source.
- 12) After the SPT from the RP to the DR at the data source end is established, data packets from the data source are transmitted to the RP along the SPT without encapsulation.
- 13) When the first multicast data packet reaches the RP along the SPT, the RP transmits the Register-Stop message to the DR at the data source end to enable the DR to stop the encapsulation of Register packets. After the DR at the data source end receives the Register-Stop message, it does not encapsulate the Register packets but transmits the Register packets to the RP along the SPT of the data source. The RP forwards the Register packets to each group member along the RPT.

Related Configuration

❖ Configuring the Transmission Interval of Join/Prune Packets

The default transmission interval of Join/Prune packets is 60 seconds.

Run the **ipv6 pim jp-timer seconds** command to set the transmission interval of Join/Prune packets.

To change the default transmission interval of Join/Prune packets, configure this command. If this command is not configured, the default transmission interval of Join/Prune packets is 60 seconds.

7.3.7 SPT Establishment

When a data packet reaches the DR connected to a group member, the DR connected to the group member transmits the Join packet in the multicast source direction to establish an SPT. Then, multicast packets are forwarded along the SPT, thereby relieving the load of the RP in the RPT and reducing the number of hops from the DR at the data source end to the receive end.

Working Principle

The SPT establishment process is as follows:

The DR at the receive end transmits the (*,G)join packet to the DR at the source end along the SPT. The (*,G)join packet is transmitted hop by hop till the DR at the source end receives the (*,G)join packet, forming an SPT.

Related Configuration

By default, SPT switching is disabled.

Run the **ipv6 pim spt-threshold [group-list ipv6_access-list]** command to configure whether to start SPT switching.

After this command is configured, when the DR receives the (S,G) packet from the first group member, one PIM Join message is generated and forwarded to the RP to establish a SPT tree. If **group-list** is defined, the defined group is switched from the RPT to the SPT. If **no** is set in this command and **group-list** is not defined, the switching from the RPT to the SPT is disabled and the device redirects to the RPT and transmits one Prune packet to the source. If **no** is set in this command, **group-list** is defined, and the defined ACL is a configured ACL, the ACL associated with **group-list** is cancelled and all groups are allowed to switch from the RPT to the SPT.

7.3.8 ASM and SSM Models

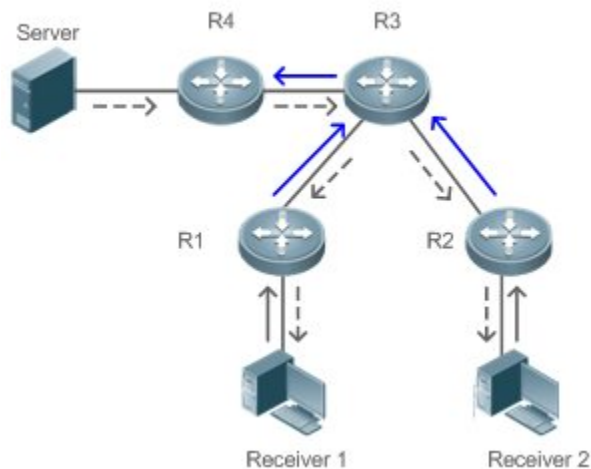
PIM-SM supports two multicast models: ASM and SSM. In the ASM model, a multicast data receiver specifies only to join a multicast group G but does not specify the multicast source S. In the SSM model, a multicast data receiver can specify both the multicast source S and multicast group G.

- When the SSM model is implemented over IPv6, MLDv2 needs to be used to manage the member relationship between hosts and devices and PIM-SMv6 needs to be used to connect devices.

In the SSM model, a multicast receiver learns about the multicast source (S,G) information by means of some channels (such as accessing the server or receiving advertisements) in advance. When the multicast receiver needs to order a multicast service, it directly transmits the MLD(S,G) Join packet to the last-hop device, for example, as shown in the following figure, Multicast Receiver 1 transmits the MLD(S,G) Join packet to order the multicast service (S,G). After receiving the MLD(S,G) Join packet from the multicast receiver, the last-hop device transmits the PIM(S,G) Join packet to the multicast source hop by hop, for example, as shown in the following figure, after receiving the MLD(S,G) Join packet from Multicast Receiver 1, R1 transmits the PIM(S,G) Join packet to R3, which transmits the PIM (S,G) Join packet to R4. As a result, the SPT from the multicast receiver to the multicast source is established.

Figure 7-5

→ MLDv2 Join → PIM(S,G) Join - - - -> Multicast Stream



The following conditions need to be met for the implementation of the SSM model:

- A multicast receiver learns about the multicast source (S,G) information beforehand by means of some channels. The multicast receiver initiates the MLD(S,G) Join packet to the desired multicast service.
- MLDv2 must be enabled on the interface of the last-hop device connected to the multicast receiver. MLDv1 does not support SSM.
- PIM-SM and SSM must be enabled on the intermediate devices between the multicast receiver and the multicast source.
- After the SSM function is enabled, the default group range of SSM is FF3x::/32. You can run a command to change the group range of SSM.

The SSM model has the following features:

- In the SSM model, a multicast receiver can learn about the multicast source information in advance by means of some channels (for example, receiving advertisements or accessing a specified server).
- The SSM model is a specific subset of PIM-SM and processes only PIM(S,G) Join and PIM(S,G) Prune messages. It discards RPT-relevant messages within the SSM range, for example, PIM(*,G) Join/Prune messages. For Register packets within the SSM range, it immediately responds with the Register-Stop packet.
- In the SSM model, no RP is required and the election and distribution of RP messages are not required. The established MDT is the SPT in SSM.

7.4 Configuration

7.4.1 Configuring Basic Functions of PIM-SMv6

Configuration Effect

- Create a PIM network to provide the IPv6 multicast service for data sources and user terminals in the network.
- Both or either of the two multicast service models (ASM and SSM) can be supported.

Notes

- PIM-SMv6 needs to use the IPv6 unicast routing function.
- If the PIM network needs to support the multicast service of the SSM model, MLDv3 or SSM Mapping needs to be configured.

Configuration Steps

- ❖ Enabling the IPv6 Multicast Routing Function
 - Mandatory.
 - The IPv6 multicast routing function should be enabled on each router unless otherwise specified.
- ❖ Enabling the PIM-SMv6 Function
 - Mandatory.
 - The PIM-SMv6 function should be enabled on the following interfaces unless otherwise specified: router interconnection interfaces, interface that function as a static RP, C-RP, or C-BSR, interface for connecting to a multicast source, and interface for connecting to a user host.
- ❖ Enabling the PIM-SMv6 PASSIVE Mode
 - In a PIM network, if an interface needs to receive only multicast data packets and does not need to participate in the establishment of the PIM network topology, the interface can be configured to work in PIM-SMv6 PASSIVE mode.
 - The PIM-SMv6 PASSIVE function should be enabled on the following interfaces unless otherwise specified: interface for connecting the stub network device to a user host. After the PIM-SMv6 PASSIVE mode is configured, this interface neither transmits nor receives PIM packets.
- ❖ Configuring an RP
 - If a PIM network needs to support the multicast service of the ASM model, an RP must be configured.
 - There are three methods of configuring an RP: configuring only a static RP, configuring only a dynamic RP, and configuring both a static RP and a dynamic RP. If both a static RP and a dynamic RP are configured, the dynamic RP is preferred.
 - Configuring a static RP: A static RP should be configured on each router unless otherwise specified.
 - Configuring a dynamic RP: A C-RP or C-BSR should be configured on one or more routers unless otherwise specified.

❖ Enabling the SSM

- If a PIM network needs to support the multicast service of the SSM model, the SSM must be enabled.
- The SSM should be enabled on each router unless otherwise specified.

Verification

Make a multicast source in the network send packets to groups within the range of ASM and SSM and make a user host join the groups.

- Check whether the user host can successfully receive packets from each group.
- Check whether correct PIM-SMv6 routing entries are created on routers.

Related Commands

❖ Enabling the IPv6 Multicast Routing Function

Command	ipv6 multicast-routing
Parameter	N/A
Description	
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Enabling the PIM-SMv6 Function

Command	ipv6 pim sparse-mode
Parameter	N/A
Description	
Command Mode	Interface configuration mode
Usage Guide	<p>Before enabling the PIM-SMv6 function, enable the multicast routing forwarding function in global configuration mode. Otherwise, multicast data packets cannot be forwarded even if the PIM-SMv6 function is enabled.</p> <p>When the PIM-SMv6 function is enabled, MLD is automatically enabled on each interface without manual configuration.</p> <p>If the message "Failed to enable PIM-SMv6 on <interface name>, resource temporarily unavailable, please try again" is displayed during the configuration of this command, try to configure this command again.</p> <p>If the message "PIM-SMv6 Configure failed! VIF limit exceeded in NSM!!!" is displayed during the configuration of this command, the configured number of multicast interfaces reaches the upper limit of multicast interfaces that can be configured on the device. If the PIM-SMv6 function still needs to be enabled on an interface, delete some unnecessary PIM-SMv6 or PIM-DMv6 interfaces.</p> <p>If an interface is of the tunnel type, only the 6Over4 configuration tunnel, 6Over4 GRE tunnel, 6Over6 configuration tunnel, and 6Over6 GRE tunnel support the IPv6 multicast function. The multicast</p>

function can also be enabled on tunnel interfaces that do not support the multicast function but no prompts are displayed and multicast packets are neither received nor transmitted.

Multicast tunnels can be established only on Ethernet ports. Embedded tunnels and QoS/ACL of multicast data are not supported.

❖ Enabling the PIM-SMv6 PASSIVE Function

Command	ipv6 pim sparse-mode passive
Parameter	N/A
Description	
Command Mode	Interface configuration mode
Usage Guide	<p>Before enabling the PIM-SMv6 function, enable the multicast routing forwarding function in global configuration mode. Otherwise, multicast data packets cannot be forwarded even if the PIM-SMv6 PASSIVE function is enabled.</p> <p>When the PIM-SMv6 function is enabled, MLD is automatically enabled on each interface without manual configuration.</p> <p>Interfaces with the PIM-SMv6 PASSIVE function enabled neither receive nor transmit PIM packets but can forward multicast packets. Therefore, the PIM-SMv6 PASSIVE mode is generally configured on the interface of the stub network device connected to a user host, so as to prevent Layer-2 flooding of PIM Hello packets.</p>

❖ Configuring a Static RP

Command	ipv6 pim rp-address <i>ipv6_rp-address</i> [<i>ipv6_access-list</i>]
Parameter	<i>ipv6_rp-address</i> : Indicates the IPv6 address of an RP.
Description	<i>ipv6_access-list</i> : References an IPv6 ACL to restrict the group address range served by the static RP. A named ACL is supported.
Command Mode	Global configuration mode
Usage Guide	<p>Multicast static RPs can be configured. A static RP and a C-RP can coexist.</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. If both the BSR mechanism and RP static configuration are effective, the dynamic configuration is preferred. 2. A control list can be used to statically configure the address of an RP for multiple multicast groups (using the ACL) or all multicast groups (without using the ACL), but one static RP address cannot be used multiple times. 3. If multiple static RPs serve the same group, the static RP with a larger IPv6 address is used preferentially. 4. Only multicast groups with the addresses allowed by the ACL are effective. By default, all multicast groups are allowed. 5. After the configuration is complete, the static RP source address will be inserted into the group range-based static RP group tree structure. The multicast static group in each group range maintains the linked list structure of one static RP group. This linked list is arranged in descending order by

	<p>IPv6 address. When an RP is selected for a group range, the RP with the largest IPv6 address will be selected.</p> <p>6. When a static RP address is deleted, this address is deleted from all existing groups and an address is selected from the existing static RP tree structure as the RP address.</p>
--	--

❖ Configuring a C-RP

Command	ipv6 pim rp-candidate <i>interface-type interface-number</i> [priority <i>priority-value</i>] [interval <i>interval-seconds</i>] [group-list <i>ipv6_access-list</i>]
Parameter Description	<p><i>interface-type interface-number</i>: Indicates an interface name. This interface address is used as the C-RP address.</p> <p>priority <i>priority-value</i>: Specifies the priority of the C-RP. The value ranges from 0 to 255 and the default value is 192.</p> <p>interval <i>seconds</i>: Indicates the interval for transmitting C-RP messages to the BSR, with the unit of seconds. The value ranges from 1 to 16,383 and the default value is 60.</p> <p>group-list <i>ipv6_access-list</i>: References an IPv6 ACL to restrict the group address range served by the C-RP. A named ACL is supported.</p>
Command Mode	Global configuration mode
Usage Guide	<p>In the PIM-SMv6 protocol, the RPT created by the multicast routing uses an RP as the root node. After the BSR is elected, all C-RPs periodically transmit C-RP messages to the BSR in unicast mode and then the BSR disperses the messages in the entire PIM domain.</p> <p>To specify an interface as the C-RP of a specific group range, contain the ACL option in this command. Note that the calculation of the group range is based only on the permitted access control entries (ACEs) and denied ACEs are not involved in the calculation.</p> <p>If group-list <i>ipv6_access-list</i> is not carried in the command, all groups are served.</p>

❖ Configuring a C-BSR

Command	ipv6 pim bsr-candidate <i>interface-type interface-number</i> [<i>hash-mask-length</i> [<i>priority-value</i>]]
Parameter Description	<p><i>interface-type interface-number</i>: Indicates an interface name. This interface address is used as the C-BSR address.</p> <p><i>hash-mask-length</i>: Indicates the hash mask length. The value ranges from 0 to 128 and the default value is 126.</p> <p><i>priority-value</i>: Indicates the priority. The value ranges from 0 to 255 and the default value is 64.</p>
Command Mode	Global configuration mode
Usage Guide	<p>A unique BSR must exist in a PIM-SMv6 domain. The BSR collects and advertises RP information. The unique well-known BSR is elected from multiple C-BSRs by means of BSMs. All C-BSRs consider that they are the BSR before knowing the BSR information. They periodically transmit BSMs that contain the BSR address and priority in the PIM-SMv6 domain.</p> <p>This command can be used to enable a device to transmit one BSM to all PIM neighbors by using the allocated BSR address. Each neighbor compares the original BSR address with the address in the received BSM. If the IPv6 address in the received BSM is equal to or larger than its BSR address, the</p>

	<p>neighbor stores this address as the BSR address and forwards the BSM. Otherwise, the neighbor discards the BSM.</p> <p>The current device deems that it is the BSR till it receives a BSM from another C-BSR and learns that the C-BSR has a higher priority (or the same priority but a larger IPv6 address).</p>
--	---

❖ Enabling the SSM

Command	<code>ipv6 pim ssm { default range ipv6_access-list }</code>
Parameter Description	<p>default: The default group address range of SSM is FF3x::/32.</p> <p>range ipv6_access-list: References an IPv6 ACL to restrict the SSM group address range. A named ACL is supported.</p>
Command Mode	Global configuration mode
Usage Guide	To apply SSM in a PIM-SMv6 network, you must configure this command.

❖ Displaying the PIM-SM Routing Table

Command	<code>show ipv6 pim sparse-mode mroute [group-or-source-address [group-or-source-address]]</code>
Parameter Description	<i>group-or-source-address:</i> Indicates the group address or source address. The two addresses cannot be group addresses or source addresses at the same time.
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	A group address, a source address, or both group address and source address can be specified each time. You can also not specify a specific group address or source address but you cannot specify two group addresses or two source addresses at the same time.

Configuration Example

❖ Creating the IPv6 Multicast Service on an IPv6 Network to Support ASM and SSM

Scenario	<p>Figure 7-6</p>
Configuration Steps	<ul style="list-style-type: none"> ➤ Configure an IPv6 unicast routing protocol (such as OSPFv6) on the routers and ensure that the unicast routes of the loopback interfaces are reachable. (Omitted) ➤ Enable the IPv6 multicast routing function on all routers.

	<ul style="list-style-type: none"> ➤ Enable the PIM-SMv6 function on device interconnection interfaces, interface for connecting to the user host, and interface for connecting to the multicast source. ➤ Configure a C-RP and a C-BSR on the loopback interfaces of Router A and Router B. Enable the PIM-SMv6 function on the loopback interfaces. ➤ Enable SSM on all routers. ➤ Enable MLDv3 on the router interface for connecting to the user host. (Omitted)
A	<pre> switch(config)#ipv6 multicast routing switch(config)#ipv6 pim ssm default switch(config)#int gi 0/2 switch(config if GigabitEthernet 0/2)#ipv6 add 2000::2/64 switch(config if GigabitEthernet 0/2)#ipv6 pim sparse mode switch(config if GigabitEthernet 0/2)#exit switch(config)#int gi 0/1 switch(config if GigabitEthernet 0/1)#ipv6 add 1000::1/64 switch(config if GigabitEthernet 0/1)#ipv6 pim sparse mode switch(config if GigabitEthernet 0/1)#exit switch(config)#int Loopback 0 switch(config if Loopback 0)#ipv6 add 3000::5/64 switch(config if Loopback 0)#ipv6 pim sparse mode switch(config if Loopback 0)#exit switch(config)#ipv6 pim rp candidate Loopback 0 </pre>
B	<pre> Qtch(config)#ipv6 multicast routing Qtch(config)#ipv6 pim ssm default Qtch(config)#int gi 0/2 Qtch(config if GigabitEthernet 0/2)#ipv6 add 2000::1/64 Qtch(config if GigabitEthernet 0/2)#ipv6 pim sparse mode Qtch(config if GigabitEthernet 0/2)#exit Qtch(config)#int gi 0/1 Qtch(config if GigabitEthernet 0/1)#ipv6 add 1100::1/64 Qtch(config if GigabitEthernet 0/1)#ipv6 pim sparse mode Qtch(config if GigabitEthernet 0/1)#exit Qtch(config)#int Loopback 0 Qtch(config if Loopback 0)#ipv6 add 5000::5/64 </pre>

	<pre>Qtech(config if Loopback 0)#ipv6 pim sparse mode Qtech(config if Loopback 0)#exit Qtech(config)#ipv6 pim bsr candidate Loopback 0</pre>
<p>Verification</p>	<p>Make Source(2000::2/64) send packets to G1(ff16::1) and make User join G1.</p> <ul style="list-style-type: none"> ➤ Check the multicast packets received by the User. The User should be able to receive multicast packets from G1. ➤ Check PIM-SMv6 routing tables on Router A and Router B. Entries should exist on the PIM-SMv6 routing tables.
<p>A</p>	<pre>switch(config)# show ipv6 pim sparse mode mroute IPv6 Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 0 (*, ff16::1) RP: 3000::5 RPF nbr: :: RPF idx: None Upstream State: JOINED 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Local 0 . . i . 1 . Joined 0 .</pre>

```
1 . . . . .
. . . . .

Asserted

0 . . . . .
. . . . .

1 . . . . .
. . . . .

FCR:

(1100::2, ff16::1)
RPF nbr: fe80::21a:a9ff:fe3a:6355
RPF idx: GigabitEthernet 0/2
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 44 seconds
kat expires in 194 seconds
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31

Local

0 . . . . .
. . . . .

1 . . . . .
. . . . .

Joined

0 . . . . .
. . . . .

1 . . . . .
. . . . .

Asserted

0 . . . . .
. . . . .

1 . . . . .
. . . . .

Outgoing
```



```
(S,G,rpt) Entries: 1
FCR Entries: 0
REG Entries: 1

(1100::2, ff16::1)
RPF nbr: ::
RPF idx: None
SPT bit: 1
Upstream State: JOINED
kat expires in 20 seconds
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31
Local
0 . . . . .
. . . . .
Joined
0 .
j . . . . .
. . . . .
Asserted
0 . . . . .
. . . . .
Outgoing
0 .
o . . . . .
. . . . .

(1100::2, ff16::1, rpt)
RP: 3000::5
RPF nbr: fe80::2d0:f8ff:fe22:341b
RPF idx: GigabitEthernet 0/2
Upstream State: RPT NOT JOINED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31
Local
```

	0

	Pruned
	0

	Outgoing
	0

Common Errors

- IPv6 unicast routing is incorrectly configured.
- IPv6 multicast routing is not enabled on a router.
- SSM is not enabled on a router or the SSM group address range of the router is different from that of other routers.
- PIM-SMv6 is not enabled on an interface (for example, interface that is specified as a C-RP or C-BSR, or interface that functions as the gateway of a user host or multicast source).
- MLDv3 is not enabled on an interface connected to a user host.
- No RP is configured in the network.
- No static RP is configured on a router or the configured static RP is different from that on other routers.
- A C-RP is configured but no C-BSR is configured in the network.
- The unicast route to the static RP, C-RP, or C-BSR is unreachable.

7.4.2 Configuring PIM Neighbor Parameters

Configuration Effect

- Negotiate about protocol parameters and adjust parameters in a Hello packet.
- PIM routers discover neighbors, negotiate about protocol parameters, and maintain neighbor relationships.
- Protect neighbor relationships to restrict neighbors.

Notes

- The basic functions of PIM-SMv6 must be configured.

Configuration Steps

- Set parameters on each PIM router interface unless otherwise specified.

Verification

Set parameters in a Hello packet on an interface and run the **debug ipv6 pim sparse-mode packet** command to check parameters in the Hello packet.

Set neighbor filtering and run the **show ipv6 pim sparse-mode neighbor** command to check the neighbor relationship.

Related Commands

❖ Configuring the Transmission Interval of Hello Messages

Command	ipv6 pim query-interval <i>seconds</i>
Parameter Description	Indicates the transmission interval of Hello packets. The unit is seconds. The value ranges from 1 to 65,535 and the default value is 30 .
Command Mode	Interface configuration mode
Usage Guide	Each time the transmission interval of Hello messages is updated, the Holdtime of Hello messages is accordingly updated according to the following rule: The Holdtime of Hello messages is updated to 3.5 times transmission interval of Hello messages. If the transmission interval of Hello messages multiplied by 3.5 is larger than 65,535, the transmission interval of Hello messages is forcibly updated to 18,725.

❖ Configuring the Propagation Delay for Hello Messages

Command	ipv6 pim propagation-delay <i>milliseconds</i>
Parameter Description	<i>milliseconds</i> : The unit is milliseconds. The value ranges from 1 to 32,767 and the default value is 500 .
Command Mode	Interface configuration mode
Usage Guide	Changing the propagation delay or prune override delay will affect J/P-override-interval. According to the protocol, J/P-override-interval must be smaller than the Holdtime of Join-Prune packets. Otherwise, short flow interruption will be incurred. This must be maintained and guaranteed by network administrators.

❖ Configuring the Prune Override Interval for Hello Messages

Command	ipv6 pim override-interval <i>milliseconds</i>
Parameter Description	<i>milliseconds</i> : The unit is milliseconds. The value ranges from 1 to 65,535 and the default value is 2500 .
Command Mode	Interface configuration mode
Usage Guide	Changing the propagation delay or prune override delay will affect J/P-override-interval. According to the protocol, J/P-override-interval must be smaller than the Holdtime of Join-Prune packets. Otherwise, short flow interruption will be incurred.

❖ Configuring the Interface Joining Suppression Capability for Hello Messages

Command	ipv6 pim neighbor-tracking
----------------	-----------------------------------

Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	When the joining suppression capability of an interface is enabled and the local router needs to transmit a Join packet to an upstream neighbor, the Join packet of the local router is suppressed and is not transmitted if the local router receives a Join packet from a neighbor to the upstream router. If the joining suppression capability of the interface is disabled, the local router transmits the Join packet. When the joining suppression capability of a downstream receiver is disabled, the upstream neighbor can accurately know the number of receivers connected to the downstream neighbor through the received Join packet, thereby implementing neighbor tracking.

❖ Configuring the Delay of Sending Out Hello Messages

Command	ipv6 pim triggered-hello-delay <i>seconds</i>
Parameter Description	<i>Seconds</i> : The unit is seconds. The value ranges from 1 to 5 and the default value is 5 .
Command Mode	Interface configuration mode
Usage Guide	When an interface is enabled or detects a new neighbor, the Triggered-Hello-Delay message is used to generate a random time period. Within the time period, the interface sends Hello packets.

❖ Configuring the DR Priority for Hello Messages

Command	ipv6 pim dr-priority <i>priority-value</i>
Parameter Description	<i>priority-value</i> : Indicates the priority. A larger value means a higher priority. The value ranges from 0 to 4,294,967,294 and the default value is 1 .
Command Mode	Interface configuration mode
Usage Guide	The process of selecting a DR is as follows: The priority parameter is set for Hello packets of devices in the same LAN. The priority is compared for the selection of a DR. The device with a higher priority is the DR. If multiple devices share the same priority, the device with a larger IP address is the DR. When the priority parameter is not set for Hello packets of a device in a LAN, the device with a larger IP address is elected as the DR in the LAN.

❖ Configuring Neighbor filtering

Command	ipv6 pim neighbor-filter <i>ipv6_access-list</i>
Parameter Description	<i>ipv6_access-list</i> : References an IPv6 ACL to restrict the neighbor address range.
Command Mode	Interface configuration mode
Usage Guide	This command can be used to filter neighbors to strengthen the security of the PIM network and restrict the address range of legitimate neighbors. If a neighbor is rejected by an ACL, PIM-SMv6 will

	not establish a peering relationship with this neighbor or suspend the peering relationship with this neighbor.
--	---

❖ Displaying Neighbor Information About an Interface

Command	show ipv6 pim sparse-mode neighbor [detail]
Parameter Description	detail: Displays details.
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	N/A

Configuration Example

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Set the transmission interval of Hello packets of PIM-SMv6 to 50 seconds. ➤ Set the propagation delay of Hello packets of PIM-SMv6 to 400 milliseconds. ➤ Set the prune override interval of Hello packets of PIM-SMv6 to 3,000 milliseconds. ➤ Configure the interface joining suppression capability for Hello messages of PIM-SMv6. ➤ Set the delay of sending out Hello messages of PIM-SMv6 to 3 seconds. ➤ Set the DR priority of Hello messages of PIM-SMv6 to 5.
	<pre> switch # configure terminal switch (config)#int gi 0/1 switch (config if GigabitEthernet 0/1)#ipv6 pim query interval 50 switch (config if GigabitEthernet 0/1)#ipv6 pim propagation delay 400 switch (config if GigabitEthernet 0/1)#ipv6 pim override interval 3000 switch (config if GigabitEthernet 0/1)#ipv6 pim triggered hello delay 3 switch (config if GigabitEthernet 0/1)# ipv6 pim dr priority 5 </pre>
Verification	Run the debug ipv6 pim sparse-mode packet command to check parameters in a Hello packet.
	<pre> switch # debug ipv6 pim sparse mode packet *Jan 2 02:37:55: %7: Hello send to GigabitEthernet 0/2 *Jan 2 02:37:55: %7: Send Hello message *Jan 2 02:37:55: %7: Holdtime: 175 *Jan 2 02:37:55: %7: T bit: off *Jan 2 02:37:55: %7: Propagation delay: 400 *Jan 2 02:37:55: %7: Override interval: 3000 *Jan 2 02:37:55: %7: DR priority: 5 *Jan 2 02:37:55: %7: Gen ID: 99572792 *Jan 2 02:37:55: %7: Secondary Addresses: *Jan 2 02:37:55: %7: 2000::2 </pre>
Configuration Steps	Configure neighbor filtering on an interface to receive neighbor packets with the address of (8000::1/64).

	<pre>switch(config if GigabitEthernet 0/2)#ipv6 pim neighbor filter acl % access list acl not exist switch(config if GigabitEthernet 0/2)#exit switch(config)#ipv6 access list acl switch(config ipv6 acl)#permit ipv6 8000::1/64 any</pre>
Verification	Before neighbor filtering is configured, display the neighbor information.
	<pre>switch#show ipv6 pim sparse mode neighbor Neighbor Address Interface Uptime/Expires DR Pri/Mode fe80::21a:a9ff:fe3a:6355 GigabitEthernet 0/2 00:32:29/00:01:16 1 /</pre>
Verification	After neighbor filtering is configured, the neighbor information is blank.
	<pre>switch#show ipv6 pim sparse mode neighbor</pre>

Common Errors

- The basic functions of PIM-SMv6 are not configured or fail to be configured.

7.4.3 Configuring BSR Parameters

Configuration Effect

- Restrict the range of BSMs.

Notes

- The basic functions of PIM-SMv6 must be configured.
- A C-RP and a C-BSR must be configured.
- The border must be configured on the interface between domains.

Configuration Steps

- ❖ Configuring the Border
 - The border must be configured if there are multiple domains.
 - Configure the border the interface between two domains.
- ❖ Configuring a PIM Router to Restrict BSMs
 - Optional.
 - This configuration can be performed on a PIM router unless otherwise specified.

- ❖ Configuring a C-BSR to Restrict the C-PR Range
 - Optional.
 - This configuration can be performed on all C-BSRs unless otherwise specified.
- ❖ Configuring a C-BSR to Receive C-RP-ADV Packets with prefix-count of 0
 - Optional.
 - This configuration can be performed on all C-BSRs unless otherwise specified.

Verification

- ❖ Verifying the Border

Enable the basic functions of PIM-SMv6, set two routers in different domains, and set Router B as a C-BSR. Router A can normally receive BSMs.

Set the common border between Router A and Router B as a border interface. Router A cannot receive BSMs.

- ❖ Verifying a PIM Router to Restrict BSMs

Enable the basic functions of PIM-SMv6 and set Router B as a C-BSR. Router A can normally receive BSMs. Restrict the C-BSR range on Router A. Router A cannot receive BSMs.

- ❖ Verifying a C-BSR to Restrict the C-PR Range

Enable the basic functions of PIM-SMv6, set Router B as a C-BSR, set Router A as a C-RP, and restrict the C-RP range on the C-BSR. Router B cannot receive packets from the C-RP.

Related Commands

- ❖ Configuring the BSR Border

Command	<code>ipv6 pim bsr-border</code>
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	The BSR border can be configured on an interface to restrict flooding of BSMs. When this interface receives BSMs, it immediately discards them and BSMs are not forwarded by this interface.

- ❖ Configuring a PIM Router to Restrict BSMs

Command	<code>ipv6 pim accept-bsr list <i>ipv6_access-list</i></code>
Parameter Description	<code>list <i>ipv6_access-list</i></code> : References an IPv6 ACL to restrict the BSR address range. A named ACL is supported.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring a C-BSR to Restrict the C-PR Range

Command	ipv6 pim accept-crp list <i>ipv6_access-list</i>
Parameter Description	list <i>ipv6_access-list</i> : References an IPv6 ACL to restrict the address range of the C-RP and the group address range served by the C-RP. A named ACL is supported.
Command Mode	Global configuration mode
Usage Guide	Configure this command on a C-BSR. When this C-BSR is elected as the BSR, it can restrict the address range of the valid C-RP and the multicast group range served by the C-RP.

❖ Displaying BSMs

Command	show ipv6 pim sparse-mode bsr-router
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	N/A

❖ Displaying All RPs Configured on the Local Device and the Multicast Groups Served by the RPs

Command	show ipv6 pim sparse-mode rp mapping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	N/A

Configuration Example

❖ Configuring the BSR Border

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Configure the BSR border on the juncture interface between Router B and Router A.
	<pre>Qtech(config if GigabitEthernet 0/2)#ipv6 pim bsr border</pre>
Verification	<p>Before the BSR border is configured, the BSM information of Router A is displayed as follows:</p>
	<pre>switch#show ipv6 pim sparse mode bsr router PIMv2 Bootstrap information BSR address: 5000::5 Uptime: 00:05:42, BSR Priority: 64, Hash mask length: 126 Expires: 00:01:28 Role: Non candidate BSR Priority: 0, Hash mask length: 126 State: Accept Preferred Candidate RP: 3000::5(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:24 switch#</pre>
	<p>Candidate RP: Indicates all C-RPs configured on the local router, excluding other routers.</p>
	<p>After the BSR border is configured, the BSM information of Router A is displayed as follows:</p>
	<pre>switch#show ipv6 pim sparse mode bsr router Candidate RP: 3000::5(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:53</pre>

❖ Configuring a PIM Router to Restrict the Source Address Range of BSMs to (8000::5/64)

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Configure PIM Router A to restrict BSMs. The restricted source address range is (8000::5/64).
	<pre>switch(config)#ipv6 access list acl switch(config ipv6 acl)#permit ipv6 8000::5/64 any switch(config ipv6 acl)#exit switch(config)#ipv6 pim accept crp list acl</pre>
Verification	Before the BSM restriction is configured, the BSM information of Router A is displayed as follows:
	<pre>switch#show ipv6 pim sparse mode bsr router PIMv2 Bootstrap information BSR address: 5000::5 Uptime: 00:05:42, BSR Priority: 64, Hash mask length: 126 Expires: 00:01:28 Role: Non candidate BSR Priority: 0, Hash mask length: 126 State: Accept Preferred Candidate RP: 3000::5(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:24 switch#</pre>
	After the BSM restriction is configured, the BSM information of Router A is displayed as follows:
	<pre>switch#show ipv6 pim sparse mode bsr router Candidate RP: 3000::5(Loopback 0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:34</pre>

❖ **Configuring a C-BSR to Restrict the Source Address Range of C-PR Packets to (9000::5/64)**

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Configure Router B to restrict C-RP packets. The restricted source address range is (9000::5/64).
	<pre>Qtech(config)#ipv6 access list acl Qtech(config ipv6 acl)#permit ipv6 9000::5/64 any Qtech(config ipv6 acl)#exit Qtech(config)#ipv6 pim accept crp list acl</pre>
Verification	<p>Before C-RP packet filtering is configured, information about all RP groups on Router B is displayed as follows:</p>
	<pre>Qtech#show ipv6 pim sparse mode rp mapping PIM Group to RP Mappings This system is the Bootstrap Router (v2) Group(s): ff00::/8 RP: 3000::5(Not self) Info source: 3000::5, via bootstrap, priority 192 Uptime: 00:02:26, expires: 00:02:08 Qtech#</pre>
	<p>After C-RP packet filtering is configured, information about all RP groups on Router B is displayed as follows:</p>
	<pre>Qtech#show ipv6 pim sparse mode rp mapping PIM Group to RP Mappings This system is the Bootstrap Router (v2)</pre>

❖ Configuring the Static RP First

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Set the address of Interface Loopback0 of Router A to 3000::5. (Omitted) ➤ Set the address of Interface Loopback1 of Router A to 4000::5. (Omitted) ➤ Set the static address of Router A to 3300::5. (Omitted) ➤ Set the static address of Router B to 3300::5. ➤ Configure the static RP first on Router A.
	<pre>switch(config)#ipv6 pim rp address 3300::5 switch(config)#ipv6 pim static rp preferred</pre>
Verification	Before static RP first is configured, display information about the RP corresponding to FF16::1.
	<pre>switch#show ipv6 pim sparse mode rp ff16::1 RP: 4000::5 Info source: 5000::5, via bootstrap PIMv2 Hash Value 126 RP 4000::5, via bootstrap, priority 56, hash value 892666309 RP 3000::5, via bootstrap, priority 200, hash value 1161101765 RP 3300::5, static (hash value 204800453 not used)</pre>
Verification	After static RP first is configured, display information about the RP corresponding to FF16::1.
	<pre>switch(config)#show ipv6 pim sparse mode rp ff16::1 RP: 3300::5 (Static) PIMv2 STATIC RP PREFERRED PIMv2 Hash Value 126 RP 4000::5, via bootstrap, priority 56, hash value 892666309 RP 3000::5, via bootstrap, priority 200, hash value 1161101765 RP 3300::5, static (hash value 204800453 not used) switch(config)#</pre>

Common Errors

- The basic functions of PIM-SMv6 are not configured or fail to be configured.
- No C-BSR is configured.
- The BSR border is not configured on an interface between different domains.

7.4.4 Configuring RP and DR Parameters

Configuration Effect

- Configure the ignorance of the C-RP priority for the RP reselection.
- Configure the DR at the data source end to detect the RP reachability.
- Restrict the (S,G) multicast group address of the data source so that the ASM model provides the multicast service only for multicast packets within the allowable range.
- Configure the rate limit for the DR at the data source end to transmit Register packets.
- Configure the checksum length of Register packets.
- Configure the source address of Register packets.
- Configure the suppression time of Register packets.
- Configure the probing time of NULL packets.
- Configure the TTL of Register packets received by the RP from the (S,G) multicast group address.
- Configure the static RP first.

Notes

- The basic functions of PIM-SMv6 must be configured.

Configuration Steps

- ❖ Configuring the Ignorance of the C-RP Priority for the RP Reselection
 - Optional.
 - The ignorance of the C-RP priority can be enabled on each router unless otherwise specified.
- ❖ Configuring the DR at the Data Source End to Detect the RP Reachability
 - Optional.
 - The reachability detection can be enabled on the DR that is directly connected to the data source unless otherwise specified.
- ❖ Restricting the (S,G) Address Range of Register Packets at the Data Source End
 - Optional.
 - The (S,G) address range of Register packets at the data source end can be restricted on all routers that function as C-RPs or static RPs unless otherwise specified.
- ❖ Restricting the Rate for the DR at the Data Source End to Transmit Register Packets
 - Optional.
 - The transmission rate limit of Register packets can be enabled on the DR that is directly connected to the data source unless otherwise specified.

- ❖ Configuring the Checksum Length of Register Packets
 - Optional.
 - The checksum length of Register packets can be configured on all C-RPs or static RPs unless otherwise specified.
- ❖ Configuring the Source Address of Register Packets
 - Optional.
 - The source address of Register packets can be configured on the DR that is directly connected to the data source unless otherwise specified.
- ❖ Configuring the Suppression Time of Register Packets
 - Optional.
 - The suppression time of Register packets can be configured on the DR that is directly connected to the data source unless otherwise specified.
- ❖ Configuring the Probing Time of NULL Packets
 - Optional.
 - The probing time of NULL packets can be configured on the DR that is directly connected to the data source unless otherwise specified.
- ❖ Configuring the TTL of Register Packets Received by the RP from the (S,G) Multicast Group Address
 - Optional.
 - The TTL of Register packets from the (S,G) multicast group address can be configured on all routers that function as C-RPs or static RPs unless otherwise specified.
- ❖ Configuring the Static RP First
 - Optional.
 - The static RP first can be configured on all routers unless otherwise specified.

Verification

- ❖ Verifying the Ignorance of the C-RP Priority

Set the address to 3000::5 and priority to 200 for Interface Loopback0 on Router A. Set the address to 4000::5 and priority to 56 for Interface Loopback1 on Router A. Set the C-BSR address to 5000::5 on Router B.

- Run the **show ipv6 pim sparse-mode rp ff16::2** command to display information about the RP that serves the current group.
- ❖ Verifying the DR at the Data Source End to Detect the RP Reachability

Set the address to 3000::5 and priority to 200 for Interface Loopback0 on Router A. Set the address to 4000::5 and priority to 56 for Interface Loopback1 on Router A. Set the C-BSR address to 5000::5 on Router B. Configure the RP reachability detection on Router B.

➤ Run the **show running-config** command to check whether the RP reachability detection is configured.

❖ Verifying the Restriction of the (S,G) Address Range of Register Packets at the Data Source End

Set the address to 3000::5 and priority to 200 for Interface Loopback0 on Router A. Set the address to 4000::5 and priority to 56 for Interface Loopback1 on Router A. Set the C-BSR address to 5000::5 on Router B. The address of the multicast group is FF16::2. Set Router A to receive packets only from the multicast source with the source address of (1300::1/64).

➤ Run the **show ip pim sparse-mode mroute** command to display the (S,G) entries.

❖ Verifying the Rate Limit for the DR at the Data Source End to Transmit Register Packets

➤ Set the rate of transmitting Register packets for Router B and then run the **show ip pim sparse-mode track** command to check the number of transmitted Register packets for confirmation.

❖ Verifying the Checksum Length of Register Packets

➤ Set Router A to check a Register packet based on the entire packet rather than based only on the packet header and Register packet header. Run the **show running-config** command to check the configuration.

❖ Verifying the Source Address of Register Packets

➤ Configure the source address of Register packets on Router B and run the **show running-config** command to check the configuration on Router A.

❖ Verifying the Suppression Time and Probing Time of Register Packets

➤ Configure the suppression time and probing time of Register packets on Router B and run the **show running-config** command to check the configuration.

❖ Verifying the TTL of Register Packets Received by the RP from the (S,G) Multicast Group Address

➤ Configure the TTL of Register packets from the (S,G) multicast group address on Router A and run the **show ip pim sparse-mode mroute** command to display the maximum (S,G) TTL.

❖ Verifying the Static RP First

➤ Configure a static RP and a C-RP on Router A, configure the static RP first, and then run the **show ipv6 pim sparse-mode rp ff16::2** command to display information about the current RP.

Related Commands

❖ Ignoring the C-RP Priority

Command	ipv6 pim ignore-rp-set-priority
---------	---------------------------------

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Displaying Information About the RP That Serves a Group

Command	show ipv6 pim sparse-mode rp-hash <i>group-address</i>
Parameter Description	<i>group-address</i> : Indicates the parsed group address.
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	N/A

❖ Configuring the DR Directly Connected to the Data Source to Detect RP Reachability

Command	ipv6 pim register-rp-reachability
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After this command is configured, the RP reachability is detected before Register packets are transmitted. If the RP is reachable, Register packets are transmitted. If the RP is unreachable, Register packets are not transmitted.

❖ Restricting the (S,G) Address Range of Register Packets at the Data Source End

Command	ipv6 pim accept-register { list <i>ipv6_access-list</i> [route-map <i>map-name</i>] route-map <i>map-name</i> [list <i>ipv6_access-list</i>] }
Parameter Description	list <i>ipv6_access-list</i> : References an IP extended ACL to restrict the (S,G) address range. The value range is 100-199, 2000-2699, and Word. route-map <i>map-name</i> : Uses a route map to restrict the (S,G) address range.
Command Mode	Global configuration mode
Usage Guide	After this command is configured, when receiving a Register packet from an unauthorized source, the RP immediately returns the Register-Stop packet.

❖ Displaying Multicast Routing Entries

Command	show ipv6 pim sparse-mode mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]]
Parameter Description	<i>group-or-source-address</i> : Indicates the group address or source address. The two addresses cannot be group addresses or source addresses at the same time.
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide	A group address, a source address, or both addresses can be specified each time. You can also not specify a specific group address or source address but you cannot specify two group addresses or two source addresses at the same time.
--------------------	---

❖ Configuring the Rate Limit for the DR to Transmit Register Packets

Command	ipv6 pim register-rate-limit rate
Parameter Description	<i>Rate</i> : Indicates the number of Register packets that are allowed to be transmitted per second. The value ranges from 1 to 65,535.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the transmission rate of Register packets from the (S,G) multicast group address rather than the Register packets of the entire system. After this command is configured, the load of the source DR and RP will be relieved and Register packets whose rate does not exceed the limit will be transmitted.

❖ Displaying the Statistics on PIM Packets

Command	show ipv6 pim sparse-mode track
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	When the system is started, the statistics start time point is first set. Each time clear ip pim sparse-mode track is called, the statistics start time point is set again and the PIM packet counter is cleared.

❖ Configuring the Checksum Calculation of a Register Packet Based on the Entire Packet

Command	ipv6 pim register-checksum-wholepkt [group-list ipv6_access-list]
Parameter Description	group-list access-list : Uses an ACL to restrict the group addresses that use this configuration. <i>access-list</i> : Supports digits <1,99> and <1300,1999>. A named ACL is supported.
Command Mode	Global configuration mode
Usage Guide	The device calculates the checksum of a Register packet based on the entire PIM protocol packet including the encapsulated multicast data packet, rather than the PIM header of the Register packet. If group-list ipv6_access-list is not carried in this command, all group addresses apply this configuration.

❖ Configuring the Source Address of Register Packets

Command	ipv6 pim register-source { ipv6_local_address interface-type interface-number }
Parameter Description	<i>local_address</i> : Specifies an IPv6 address as the source address of Register packets. <i>interface-type interface-number</i> : Specifies the IPv6 address of an interface as the source address of Register packets.
Command Mode	Global configuration mode

Usage Guide	The configured address must be reachable. When the RP receives a Register packet, it transmits the Register-Stop packet with the source IPv6 address of the Register packet as the destination address. PIM-SMv6 does not need to be enabled on associated interfaces.
--------------------	--

❖ Configuring the Suppression Time of Register Packets

Command	ipv6 pim register-suppression <i>seconds</i>
Parameter Description	<i>Seconds</i> : Indicates the suppression time of Register packets. The unit is seconds. The value ranges from 1 to 65,535 and the default value is 60 .
Command Mode	Global configuration mode
Usage Guide	Configuring this value on the DR will change the suppression time of Register packets defined on the DR. If the ipv6 pim rp-register-kat command is not configured, configuring this value on the RP will change the keepalive time of the RP.

❖ Configuring the Probing Time of Register Packets

Command	ipv6 pim probe-interval <i>seconds</i>
Parameter Description	<i>Seconds</i> : Indicates the probing time of Register packets. The unit is seconds. The value ranges from 1 to 65,535 and the default value is 5 .
Command Mode	Global configuration mode
Usage Guide	Probing time of Register packets is the interval for the source DR to transmit the NULL-Register packet to the RP prior to the timeout of the suppression time of Register packets. The probing time of Register packets cannot be larger than half of the suppression time of Register packets. Otherwise, the configuration fails and a warning is displayed. In addition, the suppression time of Register packets multiplied by three plus the probing time of Register packets cannot be larger than 65,535. Otherwise, a warning will be displayed.

❖ Configuring the KAT Interval on the RP

Command	ipv6 pim rp-register-kat <i>seconds</i>
Parameter Description	<i>Seconds</i> : Indicates the time of the KAT timer. The unit is seconds. The value ranges from 1 to 65,535 and the default value is 210 .
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring the Static RP First

Command	ipv6 pim static-rp-preferred
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After this command is configured, the priority of the static RP is higher than that of the RP elected by using the BSR mechanism.

Configuration Example

❖ Configuring Whether the C-RP Priority Is Considered for the Group-to-RP Mapping

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Set the address to 3000::5 and priority to 200 for Interface Loopback0 on Router A. (Omitted) ➤ Set the address to 4000::5 and priority to 56 for Interface Loopback1 on Router A. (Omitted) ➤ Set the C-BSR address to 5000::5 on Router B. (Omitted) ➤ Display the group corresponding to FF16::1. ➤ Configure the ignorance of C-RP priority on Router B.
	<pre>switch#configure terminal Qtech(config)# ipv6 pim ignore rp set priority</pre>
Verification	Before the ignorance of the C-RP priority is configured, the following information is displayed:
	<pre>switch(config)#show ipv6 pim sparse mode rp FF16::1 RP: 4000::5 Info source: 5000::5, via bootstrap PIMv2 Hash Value 126 RP 4000::5, via bootstrap, priority 56, hash value 892666309 RP 3000::5, via bootstrap, priority 200, hash value 1161101765</pre>
	After the ignorance of the C-RP priority is configured, the following information is displayed:
	<pre>switch(config)#show ipv6 pim sparse mode rp FF16::1 RP: 3000::5 Info source: 5000::5, via bootstrap</pre>

❖ Configuring the Reachability Detection of the RP Directly Connected to the Data Source

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Configure the reachability detection of the RP directly connected to the data source.
	<pre>Qtech(config)#ipv6 pim register-rp-reachability</pre>
Verification	Run the show running-config command to check the configuration. The following information is displayed:
	<pre>Qtech(config)#show running config !</pre>

```

!
!
ipv6 pim register rp reachability
ipv6 pim bsr candidate Loopback 0
!
!

```

❖ Restricting the (S,G) Address Range of Register Packets at the Data Source End

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Set Router A to filter packets by source address and receive packets only from the source address (1300::1/64).
	<pre> switch(config)#ipv6 pim accept register list acl % access list 101 not exist switch(config)#ipv6 access list acl switch(config ipv6 acl)#permit ipv6 1300::1/64 any switch(config ipv6 acl)#exit </pre>
Verification	<p>Before the (S,G) address range of Register packets at the data source end is restricted, run the show ipv6 pim sparse-mode mroute command to display multicast entries. The (S,G) entry and (S,G,RPT) entry exist.</p>
	<pre> switch#show ipv6 pim sparse mode mroute IPv6 Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 0 (*, ff16::1) RP: 4000::5 RPF nbr: :: RPF idx: None Upstream State: JOINED </pre>


```
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 1
FCR Entries: 0
REG Entries: 0

(*, ff16::1)
RP: 4000::5
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31
Local
0 . . .
i . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . .

Joined
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . .

Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . .

FCR:

(1100::2, ff16::1, rpt)
RP: 4000::5
```

```
RPF nbr: ::
RPF idx: None
Upstream State: PRUNED
 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31
Local
0 . . . . .
. . . . .
```

❖ Restricting the Rate for the DR at the Data Source End to Transmit Register Packets

<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Check the number of PIM packets transmitted by Router B. ➤ Check the number of PIM packets transmitted by Router B one second later. ➤ Set the rate for Router B to transmit Register packets. ➤ Check the number of PIM packets transmitted by Router B one second later.
	<pre>Qtech(config)#ipv6 pim register rate limit 1</pre>
<p>Verification</p>	<p>Before the rate limit is configured, check the number of PIM packets transmitted by the DR. The following information is displayed:</p>
	<pre>Qtech#show ipv6 pim sparse mode track PIMv6 packet counters track Elapsed time since counters cleared: 17:14:54 received sent Valid PIMv6 packets: 5064 7727 Hello: 1329 4057 Join Prune: 863 0 Register: 0 2636 Register Stop: 975 0 Assert: 0 0 BSM: 0 1034 C RP ADV: 1897 0 PIMDM Graft: 0 PIMDM Graft Ack: 0 PIMDM State Refresh: 0</pre>

<pre>Unknown PIM Type: 0 Errors: Malformed packets: 0 Bad checksums: 0 Send errors: 5 Packets received with unknown PIM version: 0</pre>
<p>Before the rate limit is configured, check the number of PIM packets transmitted by the DR one second later. The following information is displayed:</p>
<pre>Qtech#show ipv6 pim sparse mode track PIMv6 packet counters track Elapsed time since counters cleared: 17:14:55 received sent Valid PIMv6 packets: 5064 7727 Hello: 1335 4063 Join Prune: 866 0 Register: 0 2639 Register Stop: 978 0 Assert: 0 0 BSM: 0 1035 C RP ADV: 1897 0 PIMDM Graft: 0 PIMDM Graft Ack: 0 PIMDM State Refresh: 0 Unknown PIM Type: 0 Errors: Malformed packets: 0 Bad checksums: 0 Send errors: 5 Packets received with unknown PIM version: 0</pre>
<p>After the rate limit is configured, check the number of PIM packets transmitted by the DR. The following information is displayed:</p>

```

Qttech#show ipv6 pim sparse mode track
PIMv6 packet counters track
Elapsed time since counters cleared: 17:14:56

                received                sent
Valid PIMv6 packets:   5064                7727
Hello:                  1341                4069
Join Prune:             869                  0
Register:               0                  2640
Register Stop:         979                  0
Assert:                 0                  0
BSM:                   0                  1036
C RP ADV:              1897                0
PIMDM Graft:           0
PIMDM Graft Ack:       0
PIMDM State Refresh:  0
Unknown PIM Type:     0

Errors:
Malformed packets:                0
Bad checksums:                    0
Send errors:                       5
Packets received with unknown PIM version: 0
    
```

❖ Configuring the Checksum Length of Register Packets

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Configure the checksum calculation of a Register packet based on the entire packet on Router A. ➤ Run the show running-config command to check the configuration.
	<pre> switch(config)#ipv6 pim register checksum wholepkt switch(config)#show running config </pre>
Verification	Check the configuration on Router A. The configuration is displayed as follows:
	<pre> ! ! </pre>

```

ipv6 pim register checksum wholepkt
ipv6 pim rp candidate Loopback 0 priority 200
ipv6 pim rp candidate Loopback 1 priority 56
ipv6 pim ssm default
!
!
```

❖ Configuring the Source Address of Register Packets

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Set the source address of Interface Loopback1 to 5500::5/64 on Router B. (Omitted) ➤ Set the source address of Register packets to the address of Interface Loopback2 on Router B. (Omitted) ➤ Run the show running-config command to check the configuration.
	<pre>Qtech(config)#ipv6 pim register-source Loopback 1</pre>
Verification	Check the configuration on Router B.
	<pre> ! ! ipv6 pim register source Loopback 1 ipv6 pim register rate limit 1 ipv6 pim bsr candidate Loopback 0 ! !</pre>

❖ Configuring the Suppression Time and Probing Time of Register Packets

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Set the suppression time to 20 seconds on Router B. ➤ Set the probing time to 2 seconds on Router B. ➤ Run the show running-config command to check the configuration.
	<pre> Qtech(config)#ipv6 pim register suppression 20 Qtech(config)#ipv6 pim probe interval 2 Qtech(config)# show ip pim sparse mode track</pre>
Verification	Check the configuration on Router B.
	<pre> ! ipv6 pim register source Loopback 1</pre>


```

ipv6 pim register rate limit 1
ipv6 pim register suppression 20
ipv6 pim probe interval 2
ipv6 pim bsr candidate Loopback 0
!
!

```

❖ Configuring the TTL of Register Packets Received by the RP from the (S,G) Multicast Group Address

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Set the TTL of Register packets received by Router A from the (S,G) multicast group address to 60 seconds. ➤ Run the show ip pim sparse-mode mroute command to check the number of Register packets.
	<pre>Qtech(config)#ip pim rp register kat 60</pre>
Verification	<p>After the TTL is configured, check the TTL of Register packets from the (S,G) multicast group address on Router A. The TTL is not larger than 60 seconds.</p>
	<pre> switch(config)#show ipv6 pim sparse mode mroute IPv6 Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 0 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 0 (1100::2, ff16::1) RPF nbr: fe80::21a:a9ff:fe3a:6355 RPF idx: GigabitEthernet 0/2 SPT bit: 0 Upstream State: NOT JOINED kat expires in 60 seconds 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 </pre>

```

Local
0 . . . . .
. . . . .
1 . . . . .
. . . . .

Joined
0 . . . . .
. . . . .
1 . . . . .
. . . . .

Asserted
0 . . . . .
. . . . .
1 . . . . .
. . . . .

Outgoing
0 . . . . .
. . . . .
1 . . . . .
. . . . .

(1100::2, ff16::1, rpt)
RP: 4000::5
RPF nbr: ::
RPF idx: None
    
```

Common Errors

- The basic functions of PIM-SMv6 are not configured or fail to be configured.
- The (S,G) address range of Register packets at the data source end is not restricted or fails to be configured on a C-RP or static RP.
- When the (S,G) address range of Register packets at the data source end is restricted, the referenced ACL is not configured or the source/group address range allowed by the ACL is configured incorrectly.
- The source/group address ranges allowed by C-RPs or static RPs are inconsistent.

7.4.5 Configuring the Transmission Interval of Join/Prune Packets

Configuration Effect

- Change the transmission interval of Join/Prune packets to form an RPT or SPT.

Notes

- The basic functions of PIM-SMv6 must be configured.

Configuration Steps

- Configure the transmission interval of Join/Prune packets.

Verification

Set the transmission interval of Join/Prune packets to 120 seconds on Router B. Run the **show ipv6 pim sparse-mode mroute** command to check the entry TTL.

Related Commands

- ❖ Configuring the Transmission Interval of Join/Prune Packets

Command	ipv6 pim jp-timer seconds
Parameter	<i>Seconds</i> : Indicates the transmission interval of Join/Prune packets.
Description	The unit is seconds. The value ranges from 1 to 65,535 and the default value is 60 .
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

- ❖ Configuring the Transmission Interval of Join/Prune Packets on a Router

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Configure the transmission interval of Join/Prune packets on a router.
	<pre>Qtech(config)#ip pim jp timer 120</pre>
Verification	Run the show ipv6 pim sparse-mode mroute command to check the entry. The transmission time of Join/Prune packets is not larger than 120.
	<pre>switch(config)#show ipv6 pim sparse mode mroute IPv6 Multicast Routing Table (*,*,RP) Entries: 0 (*,G) Entries: 1 (S,G) Entries: 1 (S,G,rpt) Entries: 1 FCR Entries: 0 REG Entries: 0</pre>

```
(* , ff16::1)
RP: 4000::5
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
 22 23 24 25 26 27 28 29 30 31
Local
0 . . .
i . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . .
Joined
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . .
Asserted
0 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . .
1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . .
FCR:

(1100::2, ff16::1)
RPF nbr: fe80::21a:a9ff:fe3a:6355
RPF idx: GigabitEthernet 0/2
SPT bit: 1
Upstream State: JOINED
jt_timer expires in 116 seconds
kat expires in 59 seconds
  00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21
 22 23 24 25 26 27 28 29 30 31
Local
```

```
0 . . . . .
. . . . .
```

Common Errors

- The basic functions of PIM-SMv6 are not configured or fail to be configured.

7.4.6 Configuring the Last-Hop Device to Switch from the RPT to the SPT

Configuration Effect

- Switch the last-hop device from the RPT to the SPT.

Notes

- The basic functions of PIM-SMv6 must be configured.

Configuration Steps

- Configure the last-hop device to switch from the RPT to the SPT.

Verification

Configure basic functions of PIM-SMv6, make the DR at the data source end transmit data streams to Group FF16::1, and make the receiver forcibly join the Group FF16::1 to form a RPT. The DR at the receive end forcibly performs the switching from the RPT to SPT. Check the configuration on the RP.

Related Commands

- ❖ Enabling the SPT Switching Function

Command	<code>ipv6 pim spt-threshold [group-list ipv6_access-list]</code>
Parameter Description	group-list <i>ipv6_access-list</i> : References an IPv6 ACL to restrict the group address range that allows SPT switching. <i>ipv6_access-list</i> : A named ACL is supported.
Command Mode	Global configuration mode
Usage Guide	If group-list <i>ipv6_access-list</i> parameter is not carried in this command, all multicast groups are allowed to conduct SPT switching.
	If no is set in this command, group-list is carried, and the carried ACL is a configured ACL, the restriction of the ACL associated with group-list is cancelled and all groups are allowed to switch from the RPT to the SPT.

Configuration Example

- ❖ Configuring the Last-Hop Device to Switch from the RPT to the SPT

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic functions of PIM-SMv6. (Omitted) ➤ Make the DR at the data source end transmit code streams to Group FF16::1. ➤ Make the DR at the receive end receive code streams from Group FF16::1. ➤ Configure the last-hop device to switch from the RPT to the SPT on the DR at the receive end.
	<pre>switch(config)#ipv6 pim spt threshold</pre>
Verification	Run the show running-config command to check the configuration.
	<pre>switch(config)#show running config ! ! ip pim jp timer 120 ip pim spt threshold ip pim rp candidate Loopback 0 ! !</pre>

7.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears information about the dynamic RP.	clear ipv6 pim sparse-mode bsr rp-set *
Sets the packet statistics start time again and clears the PIMv6 packet counter.	clear ipv6 pim sparse-mode track

Displaying

Description	Command
Displays details about the BSR.	show ipv6 pim sparse-mode bsr-router
Displays the PIM-SM information about an interface.	show ipv6 pim sparse-mode interface [<i>interface-type interface-number</i>] [detail]
Displays the local MLD information about a PIM-SMv6 interface.	show ipv6 pim sparse-mode local-members [<i>interface-type interface-number</i>]
Displays the PIM-SMv6 routing information.	show ipv6 pim sparse-mode mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]]
Displays the PIM-SMv6 neighbor information.	show ipv6 pim sparse-mode neighbor [detail]

Displays next hop-relevant information, including the next-hop interface ID, address, and metric.	show ipv6 pim sparse-mode nexthop
Displays all RPs configured on the local device and the groups served by the RPs.	show ipv6 pim sparse-mode rp mapping
Displays information about the RP that serves the group address.	show ipv6 pim sparse-mode rp-hash <i>ipv6-group-address</i>
Displays the number of PIM packets transmitted and received from the statistics start time to the current time.	show ipv6 pim sparse-mode track

8. CONFIGURING MSDP

8.1 Overview

Multicast Source Discovery Protocol is used to connect multiple rendezvous points (RPs) on the network and share the multicast source information among these RPs.

- Use MSDP among multiple Protocol Independent Multicast - Sparse-Mode (PIM-SM) domains to share the multicast source information of these PIM-SM domains to implement cross-domain multicast.
- Use MSDP in a PIM-SM domain to share the multicast source information of multiple RPs to implement anycast-RP.

Protocols and Standards

- RFC3618: Multicast Source Discovery Protocol(MSDP)

8.2 Applications

Application	Description
Cross-Domain Multicast	Connect multiple ASs, share the multicast resources among autonomous systems (ASs), and provide the multicast service across ASs.
Anycast-RP	Share the multicast source information among multiple RPs in a single AS.

8.2.1 Cross-Domain Multicast

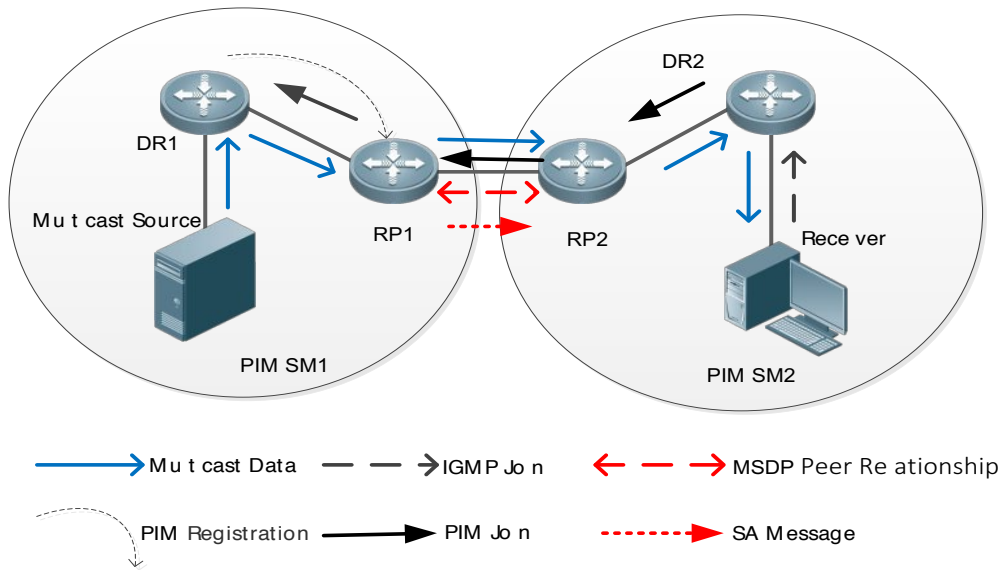
Scenario

Connect multiple ASs, run PIM-SM within the ASs, and establish an MSDP peer relationship between RPs of different ASs.

As shown in Figure 8-1, DR 1 connected to the multicast source registers with RP 1 in the local domain. DR 2 connected to the group member host triggers a join towards RP 2 in the local domain. RP 1 uses the SA message to notify RP 2 of the multicast source information. RP 2 continues to trigger a join towards the multicast source to build a multicast distribution tree (MDT).

Cross-domain multicast allows group member hosts to apply for the multicast streams across ASs.

Figure 8-1



Deployment

- Run Open Shortest Path First (OSPF) within each AS, and run Border Gateway Protocol (BGP) between ASs to implement cross-domain unicast.
- Run PIM-SM within each AS, and run MSDP between ASs to implement cross-domain multicast.

8.2.2 Anycast-RP

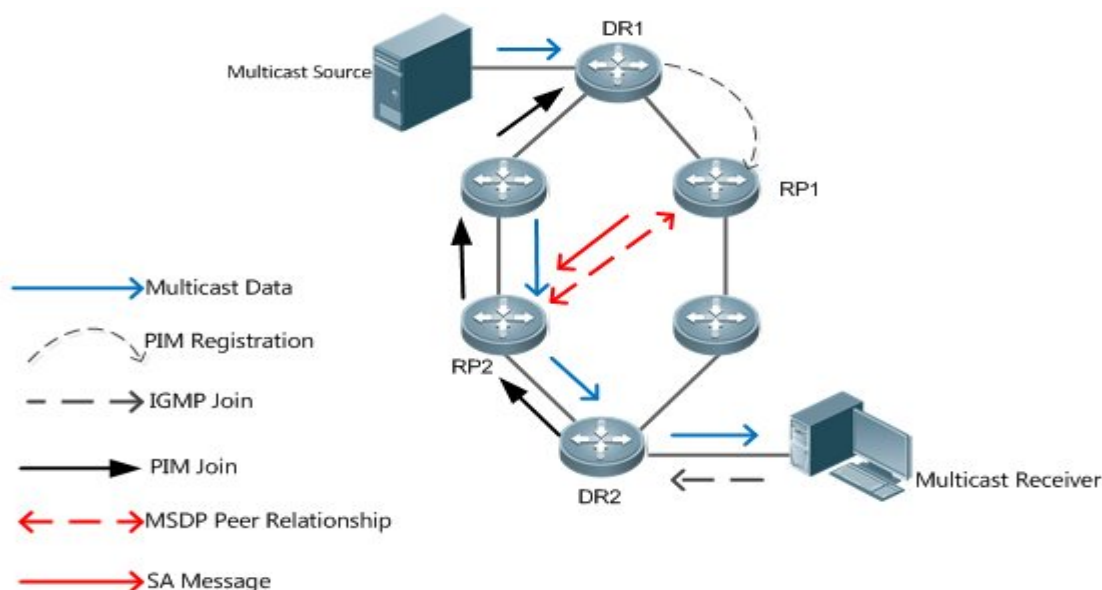
Scenario

PIM-SM runs within each AS. Multiple RPs exist, use the same RP address, and serve the same group. An MSDP peer relationship is established between these RPs.

As shown in Figure 8-2, DR 1 connected to the multicast source registers with the nearest RP 1 in the local domain. DR 2 connected to the group member host triggers a join towards the nearest RP 2. RP 1 uses the SA message to notify RP 2 of the multicast source information. RP 2 continues to trigger a join towards the multicast source to build an MDT.

Anycast-RP provides redundancy and load balancing for RPs, and helps accelerate convergence of multicast routes.

Figure 8-2



Deployment

- Run OSPF within each AS to implement intra-domain unicast.
- Run PIM-SM within each AS to implement intra-domain multicast.
- Run MSDP among RPs to share the multicast source information.

8.3 Features

Function	Description
Establishing an MSDP Peer Relationship	Connect multiple RPs to share the multicast source information.
Receiving and Forwarding SA Messages	Prevent SA flooding and suppress SA storms.

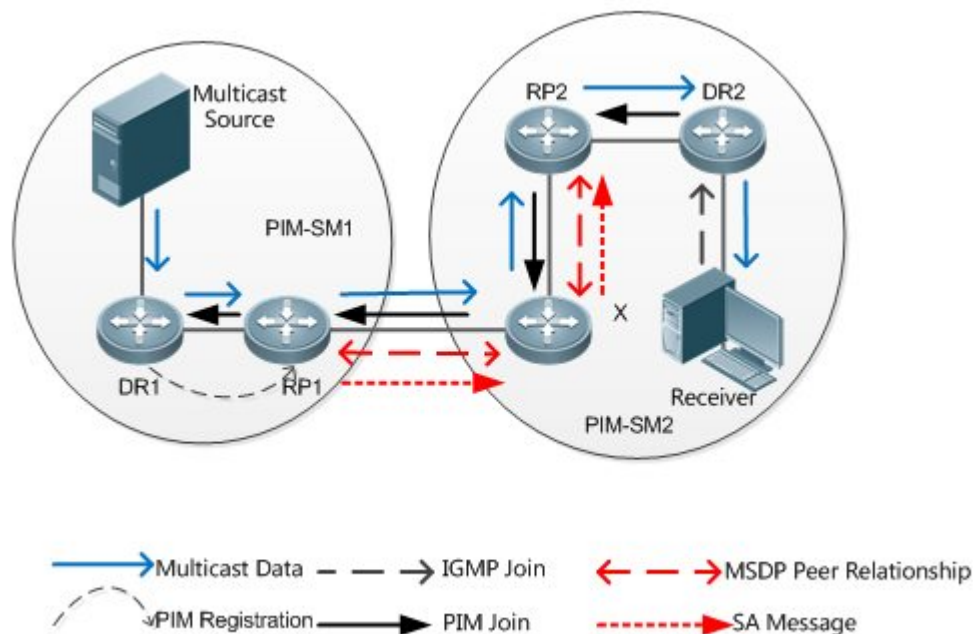
8.3.1 Establishing an MSDP Peer Relationship

Working Principle

Configure one or more pairs of MSDP peers on the network to connect RPs, thereby notifying other RPs of the multicast source information on an RP.

Use the TCP connection between MSDP peers through port 639. So far as the unicast route is reachable, the MSDP peer relationship can be established.

Figure 8-3



❖ RP Connected to the Multicast Source

Configure the MSDP peer on the RP connected to the multicast source. Then, this RP can use SA messages to send the local multicast source information to other RPs.

As shown in Figure 8-3, DR 1 registers the multicast source information with RP 1. As a peer relationship is established between RP 1 and RP 2, RP 1 sends the multicast source information to X.

❖ SA Message Forwarder

Non-RPs can also act as MSDP peers, but only forwards SA messages.

As shown in Figure 8-3, X forwards SA messages sent from RP 1 to RP 2. In this way, the multicast source information is transferred to RP 2.

❖ RP Connected to the Multicast Receiver

Configure the MSDP peer on the RP connected to the multicast receiver. Then, this RP can trigger a join towards the multicast source based on the received SA message.

As shown in Figure 8-3, DR 2 triggers a join towards RP 2. As RP 2 already obtains the multicast source information, RP 2 continues to trigger a join towards the multicast source, thus establishing an MDT from DR 1 to DR 2.

8.3.2 Receiving and Forwarding SA Messages

Working Principle

An SA message contains the multicast source address, multicast group address, and RP address. The RP address is the IP address of the RP with which the multicast source is registered.

- The RP encapsulates the locally registered multicast source information in an SA message, sends the message to all its MSDP peers.
- On receiving the SA message, each MSDP peer performs the Peer-RPF check, compares the SA-Cache, and matches the SA message against the SA incoming and outgoing filtering rules. If the SA message passes the Peer-RPF check, does not exist in the SA SA-Cache, and meets the outgoing filtering rules, this SA message is forwarded to other MSDP peers.

- The SA request and SA response messages are also used between MSDP peers to transfer source information of a specific group.

❖ Peer-RPF Check

Any SA message coming from an MSDP peer (address: N) will be checked as follows:

- Judge whether the SA message passes the Peer-RPF check in the following sequence. Once the SA message passes the Peer-RPF check, accept the SA message; otherwise, drop the SA message.

1. If N is a member of the mesh group, the SA message passes the Peer-RPF check; otherwise, go to step 2.
2. If N is the only active MSDP peer on the local device, the SA message passes the Peer-RPF check; otherwise, go to step 3.
3. If N is the RP address in the SA message, the SA message passes the Peer-RPF check; otherwise, go to step 4.
4. If an EBGP route to the RP address in the SA message exists on the local device, and the next hop of this route is N, the SA message passes the Peer-RPF check; otherwise, go to step 5.
5. If an optimum route to the RP address in the SA message exists on the local device, check as follows:

If this optimum route is a distance vector route (such as the BGP/RIP route), and this router is advertised by N, the SA message passes the Peer-RPF check.

If this optimum route is a link status route (such as the OSPF/IS-IS route), and the next hop of this router is N, the SA message passes the Peer-RPF check.

Otherwise, go to step 6.

6. If an optimum route to the RP address in the SA message exists on the local device, and this route is a MBGP/BGP route, extract the nearest AS of the AS-Path of this MBGP/BGP route. If the local device has multiple MSDP peers in this AS and N is the MSDP peer with the largest IP address, or N is the only MSDP peer in this AS, the SA message passes the Peer-RPF check; otherwise, go to step 7.

7. If N is the default MSDP peer, the SA message passes the Peer-RPF check; otherwise, go to step 8.
8. The SA message fails in the Peer-RPF check.

The Peer-RPF check helps prevent loops and SA flooding.

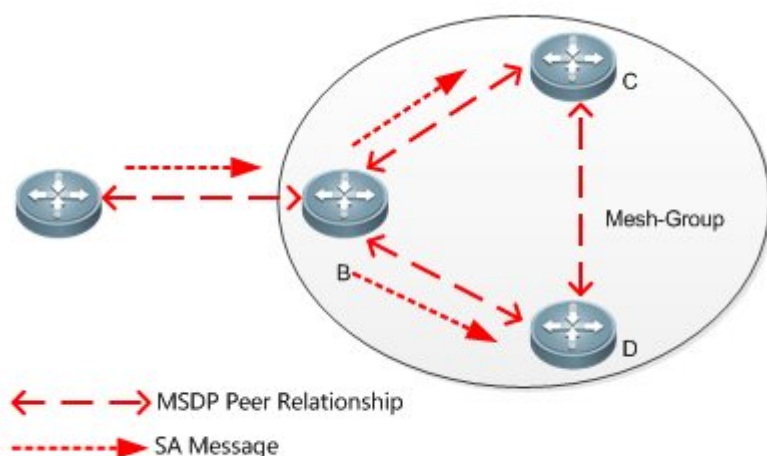
❖ Mesh Group

In a mesh group, an MSDP peer relationship is established on every two members.

- For SA messages coming from entities outside the mesh group, after passing the Peer-RPF check and SA-Cache comparison, these SA messages are forwarded to other members in the group.
- Intra-group SA messages are no longer forwarded to other members in the group.

The mesh group helps reduce the number of SA messages.

Figure 8-4



❖ SACache

The SA cache is used to buffer the SA message status. Expired SA messages will be deleted.

When an MSDP peer receives an SA message, if this message does not exist in the SA cache and passes the Peer-RPF check, the message is stored in the SA cache. If this message already exists in the SA cache, the message is ignored. This helps suppress the SA storms.

When an MSDP peer receives an SA message, if this message already exists in the SA cache, the message is immediately responded. This helps improve the protocol efficiency.

8.4 Configuration

Configuration Item	Description and Command		
Configuring Cross-Domain Multicast	<p>This configuration is mandatory in the cross-domain multicast scenario.</p>		
	<table border="1"> <tr> <td>ip msdp peer <i>peer-address</i> connect-source <i>interface-type interface-number</i></td> <td>Establishes an MSDP peer relationship.</td> </tr> </table>	ip msdp peer <i>peer-address</i> connect-source <i>interface-type interface-number</i>	Establishes an MSDP peer relationship.
ip msdp peer <i>peer-address</i> connect-source <i>interface-type interface-number</i>	Establishes an MSDP peer relationship.		
Configuring an Anycast-RP	<p>This configuration is mandatory in the Anycast-RP scenario.</p>		
	<table border="1"> <tr> <td>ip msdp peer <i>peer-address</i> connect-source <i>interface-type interface-number</i></td> <td>Establishes an MSDP peer relationship.</td> </tr> </table>	ip msdp peer <i>peer-address</i> connect-source <i>interface-type interface-number</i>	Establishes an MSDP peer relationship.
	ip msdp peer <i>peer-address</i> connect-source <i>interface-type interface-number</i>	Establishes an MSDP peer relationship.	
<table border="1"> <tr> <td>ip msdp originator-id <i>interface-type interface-number</i></td> <td>Modifies the RP address in the SA message.</td> </tr> </table>	ip msdp originator-id <i>interface-type interface-number</i>	Modifies the RP address in the SA message.	
ip msdp originator-id <i>interface-type interface-number</i>	Modifies the RP address in the SA message.		
Configuring the Peer-RPF Check Green Channel	<p>Optional. It is used to let SA message successfully pass the Peer-RPF check.</p>		
	<table border="1"> <tr> <td>ip msdp default-peer <i>peer-address</i> [prefix-list <i>prefix-list-name</i>]</td> <td>Configures the default MSDP peer.</td> </tr> </table>	ip msdp default-peer <i>peer-address</i> [prefix-list <i>prefix-list-name</i>]	Configures the default MSDP peer.
	ip msdp default-peer <i>peer-address</i> [prefix-list <i>prefix-list-name</i>]	Configures the default MSDP peer.	
<table border="1"> <tr> <td>ip msdp mesh-group <i>mesh-name peer-address</i></td> <td>Configures an MSDP mesh group.</td> </tr> </table>	ip msdp mesh-group <i>mesh-name peer-address</i>	Configures an MSDP mesh group.	
ip msdp mesh-group <i>mesh-name peer-address</i>	Configures an MSDP mesh group.		
Enabling Security Measures	<p>Optional. It is used to prevent illegal TCP connections and suppress SA storms.</p>		
	<table border="1"> <tr> <td>ip msdp password peer <i>peer-address</i> [<i>encryption-type</i>] <i>string</i></td> <td>Enables TCP MD5 encryption.</td> </tr> </table>	ip msdp password peer <i>peer-address</i> [<i>encryption-type</i>] <i>string</i>	Enables TCP MD5 encryption.
	ip msdp password peer <i>peer-address</i> [<i>encryption-type</i>] <i>string</i>	Enables TCP MD5 encryption.	
<table border="1"> <tr> <td>ip msdp sa-limit <i>peer-address sa-limit</i></td> <td>Limits the number of SA messages in the SA cache.</td> </tr> </table>	ip msdp sa-limit <i>peer-address sa-limit</i>	Limits the number of SA messages in the SA cache.	
ip msdp sa-limit <i>peer-address sa-limit</i>	Limits the number of SA messages in the SA cache.		
Restricting Broadcasting of SA Messages	<p>Optional. It is used to restrict releasing, receiving, and forwarding of SA messages.</p>		
	<table border="1"> <tr> <td>ip msdp redistribute [list <i>access-list</i>] [route-map <i>route-map</i>]</td> <td>Filters the source information released locally.</td> </tr> </table>	ip msdp redistribute [list <i>access-list</i>] [route-map <i>route-map</i>]	Filters the source information released locally.
	ip msdp redistribute [list <i>access-list</i>] [route-map <i>route-map</i>]	Filters the source information released locally.	
	<table border="1"> <tr> <td>ip msdp filter-sa-request <i>peer-address</i> [list <i>access-list</i>]</td> <td>Filters received SA requests.</td> </tr> </table>	ip msdp filter-sa-request <i>peer-address</i> [list <i>access-list</i>]	Filters received SA requests.
	ip msdp filter-sa-request <i>peer-address</i> [list <i>access-list</i>]	Filters received SA requests.	
<table border="1"> <tr> <td>ip msdp sa-filter in <i>peer-address</i> [list <i>access-list</i>] [route-map <i>route-map</i>] [rp-list <i>rp-access-list</i>] [rp-route-map <i>rp-route-map</i>]</td> <td>Filters received SA messages.</td> </tr> </table>	ip msdp sa-filter in <i>peer-address</i> [list <i>access-list</i>] [route-map <i>route-map</i>] [rp-list <i>rp-access-list</i>] [rp-route-map <i>rp-route-map</i>]	Filters received SA messages.	
ip msdp sa-filter in <i>peer-address</i> [list <i>access-list</i>] [route-map <i>route-map</i>] [rp-list <i>rp-access-list</i>] [rp-route-map <i>rp-route-map</i>]	Filters received SA messages.		
<table border="1"> <tr> <td>ip msdp sa-filter out <i>peer-address</i> [list <i>access-list</i>] [route-map <i>route-map</i>] [rp-list <i>rp-access-list</i>] [rp-route-map <i>rp-route-map</i>]</td> <td>Filters sent SA messages.</td> </tr> </table>	ip msdp sa-filter out <i>peer-address</i> [list <i>access-list</i>] [route-map <i>route-map</i>] [rp-list <i>rp-access-list</i>] [rp-route-map <i>rp-route-map</i>]	Filters sent SA messages.	
ip msdp sa-filter out <i>peer-address</i> [list <i>access-list</i>] [route-map <i>route-map</i>] [rp-list <i>rp-access-list</i>] [rp-route-map <i>rp-route-map</i>]	Filters sent SA messages.		

Configuration Item	Description and Command	
Managing MSDP Peers	Optional. It is used to conveniently manage the MSDP peer relationship.	
	<code>ip msdp description peer-address text</code>	Adds a description to an MSDP peer.
	<code>ip msdp shutdown peer-address</code>	Shuts down an MSDP peer.
Modifying Protocol Parameters	Optional. You are advised not to modify the default values of protocol parameters.	
	<code>ip msdp timer interval</code>	Modifies the TCP reconnection interval.
	<code>ip msdp ttl-threshold peer-address ttl-value</code>	Modify the TTL value of the multicast data packet carried in the SA message.

8.4.1 Configuring Cross-Domain Multicast

Configuration Effect

Establish the MSDP peer relationship between multiple ASs so that group member hosts can apply for the multicast streams across ASs.

Notes

- The inter-AC unicast route must be reachable.
- Run PIM-SM within each AS, and configure the BSR border.

Configuration Steps

- ❖ Establishing an MSDP Peer Relationship
 - Mandatory.
 - Establish a peer relationship between RPs of the corresponding multicast PIM domain.
 - Establish an MSDP peer relationship between EBGp devices of different ASs.
 - Establish an MSDP peer relationship between the RP and the EBGp device in each AS.

Command	<code>ip msdp peer peer-address connect-source interface-type interface-number</code>
Parameter Description	<i>peer-address</i> : Indicates the IP address of a remote peer. <i>interface-type interface-number</i> : Indicates the local interface, which is used to establish a TCP connection with the remote peer.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	The peer relationship is a bidirectional relationship. Therefore, this command must be configured on both sides. The IP address and local interface of the MSDP peer must be the same as those of the EBGp peer.

To ensure that SA messages can successfully pass the Peer-RPF check, you are advised to:

- Configure a mesh group.
- Configure the default MSDP peer.

Verification

Send a packet from a source (S) close to an RP to the group (G), and enable a host close to another RP to join G.

- Verify that the host can receive the (S, G) packet.
- Run the **show ip msdp summary** command on an RP in another AS to display the status of the MSDP peer.
- Run the **show ip msdp sa-cache** command on an RP in another AS to display the learned MSDP source information.

❖ Displaying the Learned MSDP Source Information

Command	show ip msdp sa-cache
Parameter	N/A
Description	
Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If no address is specified, all the (S, G) information is displayed by default.</p> <p>If an address is specified, the device checks whether this address is a unicast or multicast address. If the address is a unicast address, this address is treated as the multicast source (S), and all (S, G) information in which the multicast source is S will be displayed. If the address is a multicast address, this address is treated as the multicast group (G), and all (S, G) information in which the multicast group is G will be displayed. If this address is neither a unicast or multicast address, no information is displayed.</p> <p>If two addresses are specified, one address is treated as the multicast source (S), and the other as the multicast group (G). If one address is the unicast address, and the other address is the multicast group address, no information is displayed.</p>
	<pre> uijie# show ip msdp sa cache MSDP Source Active Cache: 2 entries (200.200.200.200, 227.1.2.2), RP: 20.20.20.20, (M)BGP/AS 100, 04:17:09/00:02:05, Peer 200.200.200.2 Learned from peer 200.200.200.2, RPF peer 200.200.200.2, SAs received: 277, Encapsulated data received: 0 (200.200.200.200, 227.1.2.3), RP: 20.20.20.20, (M)BGP/AS 100, 04:17:09/00:02:05, Peer 200.200.200.2 Learned from peer 200.200.200.2, RPF peer 200.200.200.2, SAs received: 277, Encapsulated data received: 0 </pre>

❖ Displaying the Brief MSDP Peer Information

Command	show ip msdp summary
Parameter Description	N/A
Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	N/A
<pre> Qtech# show ip msdp summary Msdp Peer Status Summary Peer Address As State Uptime/Downtime Reset Count Sa Count Peer description 200.200.200.2 100 Up 04:22:11 10 6616 No description 200.200.200.3 100 Down 19:17:13 4 0 peer A </pre>	

Configuration Example

❖ Configuring Cross-Domain Multicast

Scenario
Figure 8-5

The following table lists the interfaces and IP addresses of different devices:

Device	Interface	IP Address	Remark
A	G0/1	100.100.100.1/24	N/A
	Loopback0	10.10.10.10/32	RP address, which is used to establish an MSDP connection.
B	G0/1	100.100.100.2/24	N/A
	G0/2	1.1.1.1/24	BSR border
	Loopback0	20.20.20.20/32	Used to establish the EBGP and MSDP connections.
C	G0/1	1.1.1.2/24	BSR border
	G0/2	2.2.2.1/24	BSR border
	Loopback0	30.30.30.30/32	Used to establish the EBGP and MSDP connections.
D	G0/2	2.2.2.2/24	BSR border
	G0/1	3.3.3.1/24	N/A
	Loopback0	40.40.40.40/32	Used to establish the EBGP and MSDP connections.
E	G0/1	3.3.3.2/24	N/A
	Loopback0	50.50.50.50/32	RP address, which is used to establish an MSDP connection.

Configuration Steps

- Configure IP addresses of interfaces.
- Enable OSPF in each AS. Set up an EBGP peer relationship between AS 200 and AS 100 and between AS 200 and AS 300. Introduce BGP and OSPF to each other.
- Enable PIM-SM in each AS, configure C-BSR and C-RP, and configure the BSR border.
- Establish the MSDP peer relationship between EBGP peers and between the RP and EBGP peers.

The IP address and local interface of the MSDP peer must be the same as those of the EBGP peer.

A

```
A#configure terminal
A(config)#ip multicast routing
A(config)#interface GigabitEthernet 0/1
A(config if GigabitEthernet 0/1)#ip pim sparse mode
A(config if GigabitEthernet 0/1)# exit
A(config)#interface loopback 0
A(config if loopback 0)#ip pim sparse mode
A(config if loopback 0)# exit
A(config)#ip pim rp candidate loopback 0
```

	<pre>A(config)#ip pim bsr candidate loopback 0 A(config)#ip msdp peer 10.10.10.10 connect source loopback 0</pre>
B	<pre>B#configure terminal B(config)#ip multicast routing B(config)#interface GigabitEthernet 0/1 B(config if GigabitEthernet 0/1)#ip pim sparse mode B(config if GigabitEthernet 0/1)# exit B(config)#interface GigabitEthernet 0/2 B(config if GigabitEthernet 0/2)#ip pim sparse mode B(config if GigabitEthernet 0/2)#ip pim bsr border B(config if GigabitEthernet 0/2)# exit B(config)#interface loopback 0 B(config if loopback 0)#ip pim sparse mode B(config if loopback 0)# exit B(config)#ip msdp peer 10.10.10.10 connect source loopback 0 B(config)#ip msdp peer 30.30.30.30 connect source loopback 0</pre>
C	<pre>C#configure terminal C(config)#ip multicast routing C(config)#interface GigabitEthernet 0/1 C(config if GigabitEthernet 0/1)#ip pim sparse mode C(config if GigabitEthernet 0/1)#ip pim bsr border C(config if GigabitEthernet 0/1)# exit C(config)#interface GigabitEthernet 0/2 C(config if GigabitEthernet 0/2)#ip pim sparse mode C(config if GigabitEthernet 0/2)#ip pim bsr border C(config if GigabitEthernet 0/2)# exit C(config)#interface loopback 0 C(config if loopback 0)#ip pim sparse mode C(config if loopback 0)# exit C(config)#ip msdp peer 20.20.20.20 connect source loopback 0 C(config)#ip msdp peer 40.40.40.40 connect source loopback 0</pre>
D	<pre>D#configure terminal</pre>

	<pre>D(config)#ip multicast routing D(config)# ip pim ssmdefault D(config)#interface GigabitEthernet 0/1 D(config if GigabitEthernet 0/1)#ip pim sparse mode D(config if GigabitEthernet 0/1)# exit D(config)#interface GigabitEthernet 0/2 D(config if GigabitEthernet 0/2)#ip pim sparse mode D(config if GigabitEthernet 0/2)#ip pim bsr border D(config if GigabitEthernet 0/2)# exit D(config)#interface loopback 0 D(config if loopback 0)#ip pim sparse mode D(config if loopback 0)# exit D(config)#ip msdp peer 30.30.30.30 connect source loopback 0 D(config)#ip msdp peer 50.50.50.50 connect source loopback 0</pre>
E	<pre>E#configure terminal E(config)#ip multicast routing E(config)#interface GigabitEthernet 0/1 E(config if GigabitEthernet 0/1)#ip pim sparse mode E(config if GigabitEthernet 0/1)# exit E(config)#interface loopback 0 E(config if loopback 0)#ip pim sparse mode E(config if loopback 0)# exit E(config)#ip pim rp candidate loopback 0 E(config)#ip pim bsr candidate loopback 0 E(config)#ip msdp peer 50.50.50.50 connect source loopback 0</pre>
Verification	<p>Use the multicast source to send the packet (200.200.200.200, 225.1.1.1), and enable the host to join the group 225.1.1.1.</p> <ul style="list-style-type: none"> ➤ Verify that the host receives this packet. ➤ On device C, check the status and SA message of the MSDP peer.
D	<pre>D# show ip msdp summary Msdp Peer Status Summary Peer Address As State Uptime/Downtime Reset Count SA Count Peer Description</pre>

	<pre> 30.30.30.30 200 Up 00:01:420 1 No description D# show ip msdp sa cache MSDP Source Active Cache: 1 entries (200.200.200.200,225.1.1.1),RP:10.10.10.10,(M)BGP/AS 100, 00:00:18/00:01:57, Peer 30.30.30.30 Learned from peer 30.30.30.30, RPF peer 30.30.30.30, SAs received: 1, Encapsulated data received: 1 </pre>
--	--

Common Errors

- The BSR border is not configured, or is not configured on a correct interface.
- PIM-SM is not enabled on the local interface used to establish the MSDP peer connection or on the interface of the peer IP address.
- SA messages cannot pass the Peer-RPF check.

8.4.2 Configuring an Anycast-RP

Configuration Effect

Establish the MSDP peer relationship within an AS to provide redundancy and load balancing for RPs.

Notes

- The inter-AC unicast route must be reachable.
- PIM-SM must run within the AS, and multiple RPs using the same IP addresses must be configured.
- The C-RP and C-BSR cannot be configured on the same interface.

Configuration Steps

- ❖ Establishing an MSDP Peer Relationship
 - Mandatory.
 - Configure the following command on each RP of the same AS to establish an MSDP peer relationship with each of other RPs:

Command	<code>ip msdp peer peer-address connect-source interface-type interface-number</code>
Parameter	<i>peer-address</i> : Indicates the IP address of a remote peer.
Description	<i>interface-type interface-number</i> : Indicates the local interface, which is used to establish a TCP connection with the remote peer.
Defaults	The MSDP peer relationship is not established.

Command Mode	Global configuration mode
Usage Guide	The peer relationship is a bidirectional relationship. Therefore, this command must be configured on both sides. To ensure that SA messages can successfully pass the Peer-RPF check, you are advised to configure a mesh group.

❖ Modifying the RP Address in the SA Message

➤ Mandatory.

➤ Configure the following command on each RP of the same AS:

Command	ip msdp originator-id <i>interface-type interface-number</i>
Parameter Description	<i>interface-type interface-number</i> : Uses the IP address of this interface as the RP address in the SA message.
Defaults	By default, the RP address in the SA message is not modified.
Command Mode	Global configuration mode
Usage Guide	In the anycast-RP application scenario, the RP addresses on all RP devices are the same. If the RP address in an SA message is not modified, the RP device may determine that this SA message is sent by itself and therefore discards this message. Therefore, you need to configure different RP addresses for SA messages sent by different RP devices.

Verification

Send a packet from a source (S) close to an RP to the group (G), and enable a host close to another RP to join G.

➤ Verify that the host can receive the (S, G) packet.

➤ Run the **show ip msdp sa-cache** command on an RP in another AS to display the learned MSDP source information.

❖ Displaying the Learned MSDP Source Information

Command	show ip msdp sa-cache
Parameter Description	N/A
Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	If no address is specified, all the (S, G) information is displayed by default. If an address is specified, the device checks whether this address is a unicast or multicast address. If the address is a unicast address, this address is treated as the multicast source (S), and all (S, G) information in which the multicast source is S will be displayed. If the address is a multicast address, this address is treated as the multicast group (G), and all (S, G) information in which the multicast group is G will be displayed. If this address is neither a unicast nor multicast address, no information is displayed.

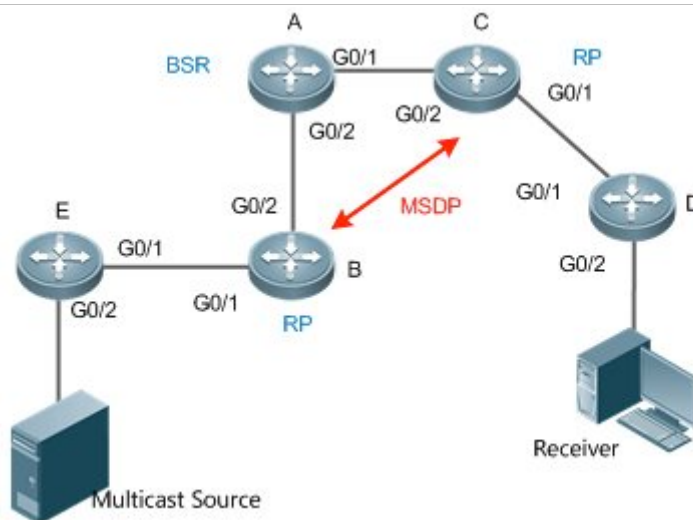
If two addresses are specified, one address is treated as the multicast source (S), and the other as the multicast group (G). If one address is the unicast address, and the other address is the multicast group address, no information is displayed.

```
Qtech# show ip msdp sa cache
MSDP Source Active Cache: 2 entries
(200.200.200.200, 227.1.2.2), RP: 20.20.20.20, (M)BGP/AS 100,
04:17:09/00:02:05, Peer 200.200.200.2
    Learned from peer 200.200.200.2, RPF peer 200.200.200.2,
    SAs received: 277, Encapsulated data received: 0
(200.200.200.200, 227.1.2.3), RP: 20.20.20.20, (M)BGP/AS 100,
04:17:09/00:02:05, Peer 200.200.200.2
    Learned from peer 200.200.200.2, RPF peer 200.200.200.2,
    SAs received: 277, Encapsulated data received: 0
```

Configuration Example

❖ Sharing the Source information Among Anycast-RPs in the Same Multicast Domain

Scenario
Figure 8-6



The following table lists the interfaces and IP addresses of different devices:

Device	Interface	IP Address	Remark
A	G0/2	2.2.2.1/24	
	G0/1	1.1.1.1/24	
	Loopback0	100.100.100.100/32	The C-BSR is configured on this interface.
B	G0/2	2.2.2.2/24	
	G0/1	3.3.3.1/24	
	Loopback1	20.20.20.20/32	Used to establish an MSDP connection and modify the RP address in the SA message.
	Loopback0	10.10.10.10/32	The C-RP is configured on this interface.
C	G0/2	1.1.1.2/24	

		G0/1	4.4.4.1/24		
		Loopback1	30.30.30.30/32	Used to establish an MSDP connection and modify the RP address in the SA message.	
		Loopback0	10.10.10.10/32	The C-RP is configured on this interface.	
	D	G0/1	4.4.4.2/24		
		G0/2	5.5.5.1/24		
	E	G0/1	3.3.3.2/24		
		G0/2	6.6.6.1/24		

Configuration Steps

- Configure IP addresses of interfaces.
- Enable OSPF within the AS.
- Enable PIM-SM within the AS, and configure the C-BSR and C-RP.
- Establish the MSDP peer relationship between RPs, and modify the RP address in the SA message.
- Configure a mesh group.

A

```
A#configure terminal
A(config)#ip multicast routing
A(config)#interface GigabitEthernet 0/1
A(config if GigabitEthernet 0/1)#ip pim sparse mode
A(config if GigabitEthernet 0/1)# exit
A(config)#interface GigabitEthernet 0/2
A(config if GigabitEthernet 0/2)#ip pim sparse mode
A(config if GigabitEthernet 0/2)# exit
A(config)#interface loopback 0
A(config if loopback 0)#ip pim sparse mode
A(config if loopback 0)# exit
A(config)#ip pim bsr candidate loopback0
```

B

```
B#configure terminal
B(config)#ip multicast routing
B(config)#interface GigabitEthernet 0/1
B(config if GigabitEthernet 0/1)#ip pim sparse mode
B(config if GigabitEthernet 0/1)# exit
B(config)#interface GigabitEthernet 0/2
B(config if GigabitEthernet 0/2)#ip pim sparse mode
B(config if GigabitEthernet 0/2)# exit
B(config)#interface loopback 0
```



```
B(config if loopback 0)#ip pim sparse mode
B(config if loopback 0)# exit
B(config)#interface loopback 1
B(config if loopback 1)#ip pim sparse mode
B(config if loopback 1)# exit
B(config)#ip pim rp candidate loopback 0
B(config)#ip msdp peer 30.30.30.30 connect source loopback 1
B(config)# ip msdp originator id loopback 1
B(config)#ip msdp mesh group mesh name 30.30.30.30
```

C

```
C#configure terminal
C(config)#ip multicast routing
C(config)#interface GigabitEthernet 0/1
C(config if GigabitEthernet 0/1)#ip pim sparse mode
C(config if GigabitEthernet 0/1)# exit
C(config)#interface GigabitEthernet 0/2
C(config if GigabitEthernet 0/2)#ip pim sparse mode
C(config if GigabitEthernet 0/2)# exit
C(config)#interface loopback 0
C(config if loopback 0)#ip pim sparse mode
C(config if loopback 0)# exit
C(config)#interface loopback 1
C(config if loopback 1)#ip pim sparse mode
C(config if loopback 1)# exit
C(config)#ip pim rp candidate loopback 0
C(config)#ip msdp peer 20.20.20.20 connect source loopback 1
C(config)# ip msdp originator id loopback 1
C(config)#ip msdp mesh group mesh name 20.20.20.20
```

D

```
D#configure terminal
D(config)#ip multicast routing
D(config)#interface GigabitEthernet 0/1
D(config if GigabitEthernet 0/1)#ip pim sparse mode
D(config if GigabitEthernet 0/1)# exit
D(config)#interface GigabitEthernet 0/2
```

	<pre>D(config if GigabitEthernet 0/2)#ip pim sparse mode D(config if GigabitEthernet 0/2)# exit</pre>
E	<pre>E#configure terminal E(config)#ip multicast routing E(config)#interface GigabitEthernet 0/1 E(config if GigabitEthernet 0/1)#ip pim sparse mode E(config if GigabitEthernet 0/1)# exit E(config)#interface GigabitEthernet 0/2 E(config if GigabitEthernet 0/2)#ip pim sparse mode E(config if GigabitEthernet 0/2)# exit</pre>
Verification	<p>Use the multicast source to send the packet (6.6.6.6,225.1.1.1), and enable the host to join the group 225.1.1.1.</p> <ul style="list-style-type: none"> ➤ Verify that the host receives this packet. ➤ On device C, check the status and SA message of the MSDP peer.
C	<pre>C# show ip msdp summary Msdp Peer Status Summary Peer Address As State Uptime/Downtime Reset Count SA Count Peer Description 20.20.20.20 Unknown Up 00:01:420 1 No description C# show ip msdp sa cache MSDP Source Active Cache: 1 entries (6.6.6.6,225.1.1.1),RP:10.10.10.10,(M)BGP/AS unknown, 00:00:18/00:01:57, Peer 20.20.20.20 Learned from peer 20.20.20.20, RPF peer 20.20.20.20,</pre>

Common Errors

- The C-BSR and C-RP are configured on the same interface.
- The RP address in the SA message is not modified.
- SA messages cannot pass the Peer-RPF check.

8.4.3 Configuring the Peer-RPF Check Green Channel

Configuration Effect

Configure the Peer-RPF check green channel so that all SA messages sent from a specified MSDP peer can pass the Peer-RPF check.

Configure an MSDP mesh group so that all SA messages sent from members of the mesh group can pass the Peer-RPF check.

Notes

- The MSDP peer relationship must be established between devices.

Configuration Steps

❖ Configuring the Default MSDP Peer

- Optional.
- On an MSDP peer, if it is not necessary to perform the Peer-RPF check on SA messages sent from a specified peer, configure this peer as the default peer.

Command	ip msdp default-peer <i>peer-address</i> [prefix-list <i>prefix-list-name</i>]
Parameter Description	<i>peer-address</i> : Indicates the IP address of a remote peer. prefix-list <i>prefix-list-name</i> : Specifies the prefix list, which is used to limit the RPs initiating SA messages.
Defaults	By default, no default peer is configured.
Command Mode	Global configuration mode
Usage Guide	If the command does not contain prefix-list <i>prefix-list-name</i> , all SA messages are accepted. If the command contains prefix-list <i>prefix-list-name</i> but the specified prefix list does not exist, all SA messages are accepted. If the command contains prefix-list <i>prefix-list-name</i> , and the specified prefix list exists, only the SA messages initiated by RPs specified in this prefix list are accepted.

❖ Creating a Mesh Group

- Optional.
- Among multiple MSDP peers, if SA messages coming from any of these peers pass the Peer-RPF check by default, you can add these peers to a mesh group.

Command	ip msdp mesh-group <i>mesh-name</i> <i>peer-address</i>
Parameter Description	<i>mesh-name</i> : Indicates the name of the mesh group. The name is case sensitive. <i>peer-address</i> : Indicates the IP address of the MSDP peer to be added to the mesh group.
Defaults	By default, no mesh group is configured.
Command Mode	Global configuration mode
Usage Guide	An MSDP peer relationship must be established between every two MSDP peers added to the same mesh group. All SA messages sent by members of the mesh group can pass the Peer-RPF check.

Verification

- Check whether SA messages sent by the default peer can pass the Peer-RPF check.
- Check the configuration of the mesh group, and check whether all SA messages sent by members of the mesh group can pass the Peer-RPF check.
- ❖ Displaying Information about the Peer-RPF Check of a Specified MSDP Peer

Command	show ip msdp rpf-peerip-address
Parameter Description	<i>peer-address</i> : Indicates the IP address of the SA message initiator.
Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	N/A
	<pre>Qtech# show ip msdp rpf peer 1.1.1.1 RPF peer information for 1.1.1.1 RPF peer: 200.200.200.2 RPF rule: Peer is only active peer RPF route/mask: Not used RPF type: Not used</pre>

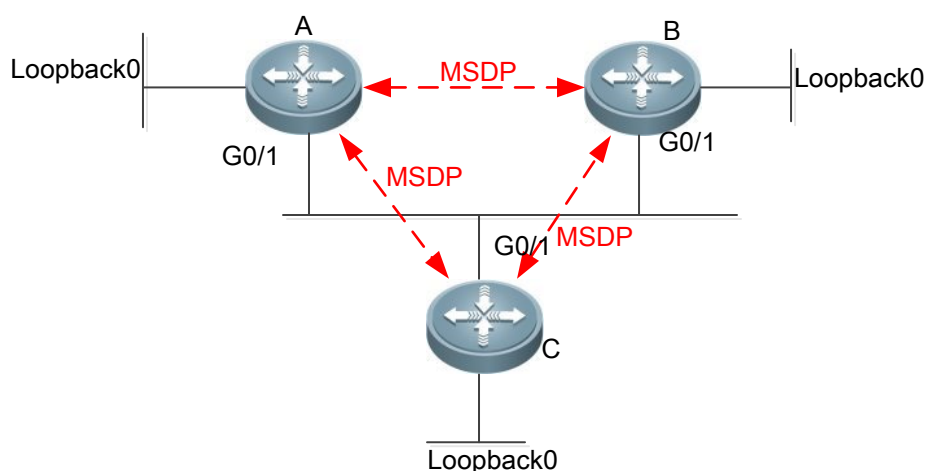
- ❖ Displaying the Mesh Group Configuration

Command	show ip msdp mesh-group
Parameter Description	N/A
Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	N/A
	<pre>Qtech# show ip msdp mesh-group MSDP peers in each Mesh group, <Mesh group name>:<# peers> msdp mesh: 1.1.1.2 1.1.1.3</pre>

Configuration Example

- ❖ Configuring the Peer-RPF Check and a Mesh Group

Figure 8-7



The following table lists the interfaces and IP addresses of different devices:

Device	Interface	IP Address	Remark
A	G0/1	20.0.0.3/24	
	Loopback0	10.1.1.1/24	
B	G0/1	20.0.0.4/24	
	Loopback0	40.0.0.1/24	
	G0/1	20.0.0.222/24	
	Loopback0	30.0.0.2/24	

Configuration Steps

- Configure IP addresses of interfaces.
- Enable OSPF within the AS.
- Establish the MSDP peer relationship between A and B and between A and C.
- Enable PIM-SM on the G0/1 interface of device C.
- Before configuration, there are two active MSDP peers on device A, but it is not known which one should be selected as the RPF peer. Therefore, display the RPF peer information. "RPF peer does not exist" is displayed.
- Configure the default MSDP peer, and check whether the configuration is successful.
- Configure a mesh group.

A

```
A#configure terminal
A(config)#ip msdp peer 20.0.0.4 connect source gi0/1
A(config)#ip msdp peer 30.0.0.2 connect source loopback 0
```

B

```
B#configure terminal
B(config)#ip msdp peer 20.0.0.3 connect source gi0/1
```

C

```
C#configure terminal
C(config)#ip msdp peer 10.0.0.1 connect source loopback 0
C(config)#interface GigabitEthernet 0/1
```

	<pre>C(config if GigabitEthernet 0/1)#ip pim sparse mode C(config if GigabitEthernet 0/1)# exit</pre>
	<ul style="list-style-type: none"> ➤ Before configuration, there are two active MSDP peers on device A, but it is not known which one should be selected as the RPF peer. Therefore, display the RPF peer information. "RPF peer does not exist" is displayed. ➤ Configure the default MSDP peer. Then, display the RPF peer information. "Peer is best default peer" is displayed.
A	<pre>A#configure terminal A(config)#ip msdp default peer 30.0.0.2</pre> <ul style="list-style-type: none"> ➤ Cancel the default peer, and send the multicast source information to device C. Information is displayed on device A, indicating that the SA message is received, but does not pass the Peer-RPF check. ➤ On device A, add 30.0.0.2 to the mesh group. Then, device A can receive the SA message normally.
A	<pre>A#configure terminal A(config)#no ip msdp default peer 30.0.0.2</pre>
A	<pre>A#configure terminal A(config)#ip msdp mesh group first 30.0.0.2</pre>
Verification	N/A

8.4.4 Enabling Security Measures

Configuration Effect

Enable MD5 encryption on TCP connections between MSDP peers to prevent illegal TCP connections. Limit the number of SA messages in the SA cache of a specified MSDP peer to suppress SA storms.

Notes

- The MSDP peer relationship must be established between devices.

Configuration Steps

- ❖ Configuring MD5 Encryption on TCP Connections Between MSDP Peers
- Optional.
- Configure consistent MD5 encryption on MSDP peers that require encryption.

Command	<code>ip msdp password peer <i>peer-address</i> [<i>encryption-type</i>] <i>string</i></code>
Parameter	<i>peer-address</i> : Indicates the IP address of a remote peer.
Description	<i>encryption-type</i> : Indicates the encryption level. Currently, only levels 0 to 7 are supported. 0 is the lowest level, and 7 is the highest level. The default value is 0. <i>string</i> : Indicates the cipher used for TCP MD5 authentication.

Defaults	By default, MD5 encryption is not configured.
Command Mode	Global configuration mode
Usage Guide	<p>To authenticate the ID of an MSDP peer, enable MD5 encryption on the TCP connection established with this MSDP peer. The MSDP peer must have the consistent configuration, and the cipher must be the same; otherwise, the connection fails.</p> <p>If the configuration or cipher changes, the local device does not stop the current session, and will attempt to use a new cipher to retain the current session until timeout.</p> <p>If the encryption level is set to 7, the cipher text length must be an even number equaling to or greater than 4; otherwise, the configuration fails.</p>

❖ Limiting the Number of SA Messages in the SA Cache of a Specified MSDP Peer

➤ Optional.

➤ Perform this configuration if you need to limit the number of SA messages in the SA cache of a specified MSDP peer.

Command	ip msdp sa-limit <i>peer-address sa-limit</i>
Parameter Description	<i>peer-address</i> : Indicates the IP address of a remote peer. <i>sa-limit</i> : Indicates the maximum number of SA messages in the SA cache.
Defaults	The default value is 1,024.
Command Mode	Global configuration mode
Usage Guide	<p>An MSDP peer relationship must be established between every two MSDP peers added to the same mesh group.</p> <p>Assume that the number of SA messages in the SA cache already exceeds the limit. After the configuration is completed, the number of SA messages in the SA cache does not exceed the limit.</p>

Verification

➤ Check the connection between peers on which MD5 encryption is configured.

➤ Send a number of source information packets that exceeds the limit to the peer where the maximum number of SA messages in the SA cache is configured. Check whether all the source information can be learned.

❖ Displaying the Number of SA Messages Learned from a Specified Peer


Command	show ip msdp count
Parameter Description	N/A
Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	N/A
	<pre>Qtech# show ip msdp count</pre>

```
SA State per Peer Counters, <Peer>: <# SA learned>
1.1.1.2      : 0
100.100.100.14 : 0
100.100.100.15 : 0
100.100.100.200: 0
200.200.200.2  : 2
200.200.200.3  : 0
200.200.200.6  : 0
200.200.200.13 : 0
200.200.200.66 : 0

SA State per ASN Counters, <asn>: <# sources>/<# groups>
Total entries: 2
100: 1/2
```

Configuration Example

- ❖ Configuring MD5 Encryption on an MSDP Peer and Limiting the Number of SA Messages Sent by This MSDP Peer in the SA Cache

<p>Scenario Figure 8-8</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Establish an MSDP peer relationship between A and B. ➤ Configure MD5 encryption on device A. ➤ After MSDP timeout, configure the MD5 cipher of the peer on device B, which is the same as the cipher on device A. Then, the session is reconnected. ➤ On device A, set the maximum number of SA messages sent by the peer 20.0.0.4 in the SA cache to 10.
<p>A</p>	<pre>A#configure A(config)# ip msdp password peer 20.0.0.4 0 1234567 A(config)# ip msdp sa limit 20.0.0.4 10</pre>
<p>B</p>	<pre>B#configure B(config)# ip msdp password peer 20.0.0.4 0 1234567</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ➤ After MD5 is configured on device A, but is not configured on device B, a message will be displayed, indicating the MD5 encryption failure. At this time, the MSDP peer is in DOWN state.

	<ul style="list-style-type: none"> ➤ A period of time after MD5 is configured on device B, the MSDP peer is in DOWN state. ➤ Send 20 multicast source packets to device B. A message will be displayed on device A, indicating that the number of SA messages exceeds the limit.
A	<pre>A# debug ip msdp sa cache A# show ip msdp count</pre>

8.4.5 Restricting Broadcasting of SA Messages

Configuration Effect

Configure the SA message filtering rules to restricting broadcasting of SA messages.

Notes

- The MSDP peer relationship must be established between devices.

Configuration Steps

❖ Filtering the Source Information Released Locally

- Optional.
- Configure the SA release filtering rule on an MSDP device where releasing of the SA information needs to be limited.

Command	ip msdp redistribute [<i>list access-list</i>] [<i>route-map route-map</i>]
Parameter Description	<i>list access-list</i> : Indicates the access control list (ACL) used to control the ranges of S and G. <i>route-map route-map</i> : Indicates the route map used to control the ranges of S and G.
Defaults	By default, no rule is configured to filter locally released SA information.
Command Mode	Global configuration mode
Usage Guide	<p>After this command is configured, only the accepted (S, G) information (either coming from the local domain or other domains) can be injected to the MSDP.</p> <p>If the command contains <i>list access-list</i>, only the (S, G) information matching this ACL can be released.</p> <p>If the command contains <i>route-map route-map</i>, only the (S, G) information matching this route map can be released.</p> <p>If the command contains both parameters, only the (S, G) information matching the ACL and route map can be released.</p> <p>If the command does not contain any parameter, no (S, G) information is released.</p>

❖ Filtering Received SA Requests

- Optional.

- Perform this configuration on the MSDP device where responding to the SA requests needs to be limited.

Command	ip msdp filter-sa-request <i>peer-address</i> [list <i>access-list</i>]
Parameter	<i>peer-address</i> : Indicates the IP address of a remote peer.
Description	list <i>access-list</i> : Indicates the ACL used to control the range of the group address.
Defaults	By default, no rule is configured to filter received SA requests.
Command Mode	Global configuration mode
Usage Guide	Use this command if you need to control the SA requests that can be accepted and responded. If the command does not contain list <i>access-list</i> , all SA requests will be ignored. If the command contains list <i>access-list</i> , but this AC does not exist, all SA requests will be ignored. If the command contains list <i>access-list</i> , and this AC exists, only the SA requests allowed by the ACL will be accepted, and others are ignored.

❖ Filtering Received SA Messages

- Optional.
- Perform this configuration on an MSDP device where the incoming SA information needs to be limited.

Command	ip msdp sa-filter in <i>peer-address</i> [list <i>access-list</i>] [route-map <i>route-map</i>] [rp-list <i>rp-access-list</i>] [rp-route-map <i>rp-route-map</i>]
Parameter Description	<i>peer-address</i> : Indicates the IP address of a remote peer. list <i>access-list</i> : Indicates the number or name of the extended IP ACL of a specified (S, G). It is used to control the multicast source information (S, G) that is allowed to pass. route-map <i>route-map</i> : Indicates the name of the route map of the specified (S, G). The multicast source information (S, G) is allowed to pass only when the AS path of the route on the S matches the AS path in the route map. rp-list <i>rp-access-list</i> : Indicates the number or name of the standard ACL of a specified RP. It is used to control the RPs, of which the multicast source information (S, G) that is allowed to pass. rp-route-map <i>rp-route-map</i> : Indicates the name of the route map of a specified RP. The multicast source information (S, G) is allowed to pass only when the AS path of the route on the RP matches the AS path in the route map.
Defaults	By default, no rule is configured to filter incoming SA messages.
Command Mode	Global configuration mode
Usage Guide	If this command is configured, but no ACL or route map is specified, all incoming SA messages will be filtered. If only one keyword (list or route-map) is specified, and every multicast source record (S, G) in the SA message meets the rule specified by the keyword, the multicast source record (S, G) will be received. If either rp-list or rp-route-map is specified, and the RP address contained in the SA message meets the rule specified by this keyword, this SA message will be received.

If two or more of the keywords (including **list**, **route-map**, **rp-list**, and **rp-route-map**) are specified, only multicast source record (S, G) in the SA message that meets the rules specified by all the available keywords can be received.

❖ Filtering Sent SA Messages

➤ Optional.

- Perform this configuration on an MSDP device where the outgoing SA information needs to be limited.

Command	ip msdp sa-filter out <i>peer-address</i> [list <i>access-list</i>] [route-map <i>route-map</i>] [rp-list <i>rp-access-list</i>] [rp-route-map <i>rp-route-map</i>]
Parameter Description	<p><i>peer-address</i>: Indicates the IP address of a remote peer.</p> <p>list <i>access-list</i>: Indicates the number or name of the extended IP ACL of the specified (S, G). It is used to control the multicast source information (S, G) that is allowed to pass.</p> <p>route-map <i>route-map</i>: Indicates the name of the route map of the specified (S, G). The multicast source information (S, G) is allowed to pass only when the AS path of the route on the S matches the AS path in the route map.</p> <p>rp-list <i>rp-access-list</i>: Indicates the number or name of the standard ACL of a specified RP. It is used to control the RPs, of which the multicast source information (S, G) that is allowed to pass.</p> <p>rp-route-map <i>rp-route-map</i>: Indicates the name of the route map of a specified RP. The multicast source information (S, G) is allowed to pass only when the AS path of the route on the RP matches the AS path in the route map.</p>
Defaults	By default, no rule is configured to filter outgoing SA messages.
Command Mode	Global configuration mode
Usage Guide	<p>If this command is configured, but no ACL or route map is specified, no SA message will be sent to this MSDP peer.</p> <p>If only one of the keywords (including list, route-map, rp-list, and rp-route-map) is specified, any multicast source record (S, G) that meets the rule specified by the keyword will be forwarded to this MSDP peer.</p> <p>If two or more of the keywords (including list, route-map, rp-list, and rp-route-map) is specified, any multicast source record (S, G) that meets the rules specified by all the available keywords will be forwarded to this MSDP peer.</p>

Verification

- Check whether SA messages initiated by the local device meet the filtering rules.
- Check whether SA messages learned by the local device meet the filtering rules.
- ❖ Displaying SA Messages Initiated by the Local Device

Command	show ip msdp sa-originated
Parameter Description	N/A

Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If the local device is the RP of PIM-SM, multicast source (S, G) information is registered on the RP, and the MSDP peer is configured on the local device, you can run this command to display the (S, G) information initiated by the local device.</p> <p>The (S, G) information displayed by this command has met the criteria specified by the redistribution command ip msdp redistribute), but such (S, G) information can be sent to the MSDP peer only when the information meets the outgoing SA information filtering rules specified by the ip msdp sa-filter out command.</p>
	<pre>Qtech# show ip msdp sa originated MSDP Source Active Originated: 5 entries (192.168.23.78, 225.0.0.1), RP: 192.168.23.249 (192.168.23.79, 225.0.0.2), RP: 192.168.23.249 (192.168.23.80, 225.0.0.3), RP: 192.168.23.249 (192.168.23.81, 225.0.0.4), RP: 192.168.23.249 (192.168.23.82, 225.0.0.5), RP: 192.168.23.249</pre>

Configuration Example

❖ Configuring Rules for Filtering Incoming or Outgoing SA Messages

<p>Scenario Figure 8-9</p>																										
	<p>The following table lists the interfaces and IP addresses of different devices:</p> <table border="1"> <thead> <tr> <th>Device</th> <th>Interface</th> <th>IP Address</th> <th>Remark</th> </tr> </thead> <tbody> <tr> <td rowspan="2">A</td> <td>G0/1</td> <td>20.0.0.3/24</td> <td></td> </tr> <tr> <td>Loopback0</td> <td>10.1.1.1/24</td> <td></td> </tr> <tr> <td rowspan="3">B</td> <td>G0/1</td> <td>20.0.0.4/24</td> <td></td> </tr> <tr> <td>Loopback0</td> <td>40.0.0.1/24</td> <td></td> </tr> <tr> <td>G0/1</td> <td>20.0.0.222/24</td> <td></td> </tr> <tr> <td></td> <td>Loopback0</td> <td>30.0.0.2/24</td> <td></td> </tr> </tbody> </table>	Device	Interface	IP Address	Remark	A	G0/1	20.0.0.3/24		Loopback0	10.1.1.1/24		B	G0/1	20.0.0.4/24		Loopback0	40.0.0.1/24		G0/1	20.0.0.222/24			Loopback0	30.0.0.2/24	
Device	Interface	IP Address	Remark																							
A	G0/1	20.0.0.3/24																								
	Loopback0	10.1.1.1/24																								
B	G0/1	20.0.0.4/24																								
	Loopback0	40.0.0.1/24																								
	G0/1	20.0.0.222/24																								
	Loopback0	30.0.0.2/24																								

Configuration Steps	<ul style="list-style-type: none"> ➤ Complete the basic configuration, as described in section 8.4.3 "Configuring the Peer-RPF Check Green Channel". ➤ Configure rules for filtering incoming SA messages on device A. ➤ Configure rules for filtering outgoing SA messages on device A. ➤ Send the multicast source information to device C.
A	<pre>A#configure A(config)# ip msdp sa filter in 30.0.0.2 A(config)# ip msdp sa filter in 30.0.0.2 list 100 A(config)# ip access list extended 100 A(config ext nacl)# permit ip host 20.0.0.100 host 225.0.0.1 A(config)# ip msdp sa filter in 30.0.0.2 rp list rp acl 1 A(config)# ip access list standard rp acl 1 A(config std nacl) # permit host 20.0.0.221 A(config)# ip msdp sa filter in 30.0.0.2 rp route map rp rm 1 A(config)# route map rp rm 1 A(config route map)#match as path 1 A(config)# ip as path access list 1 permit 2 A#configure A(config)# ip msdp sa filter out 30.0.0.2 A(config)# ip msdp sa filter out 30.0.0.2 list 101 A(config)# ip access list extended 101 A(config ext nacl)# permit ip host 20.0.0.100 host 225.0.0.1 A(config)# ip msdp sa filter out 30.0.0.2 rp list rp acl 2 A(config)# ip access list standard rp acl 2 A(config std nacl) # permit host 20.0.0.221 A(config)# ip msdp sa filter out 30.0.0.2 rp route map rp rm 2 A(config)# route map rp rm 1 A(config route map)#match as path 1 A(config)# ip as path access list 1 permit 2</pre>
Verification	<ul style="list-style-type: none"> ➤ Send the multicast source information to device C in various scenarios. ➤ On device A, check whether the learned multicast source information meets the incoming requirements. ➤ On device B, check whether the learned multicast source information meets the outgoing requirements.
A	<pre>A#show ip msdp sa cache</pre>

B	B#show ip msdp sa cache
C	B#show ip msdp sa originated

8.4.6 Managing MSDP Peers

Configuration Effect

Manage MSDP peers by adding descriptions to a specified MSDP or reset an MSDP peer.

Notes

- MSDP peers must be created in advance.

Configuration Steps

- ❖ Configuring the Description for an MSDP Peer

- Optional.

- Perform this configuration on an MSDP peer that should be managed.

Command	ip msdp description <i>peer-address text</i>
Parameter	<i>peer-address</i> : Indicates the IP address of a remote peer.
Description	<i>text</i> : Indicates the string that describes the MSDP peer.
Defaults	By default, no description information is configured of an MSDP peer.
Command Mode	Global configuration mode
Usage Guide	N/A

- ❖ Shutting Down an MSDP Peer

- Optional.

- Perform this configuration when it is required to temporarily shut down the connection with a specified peer.

Command	ip msdp shutdown <i>peer-address</i>
Parameter Description	<i>peer-address</i> : Indicates the IP address of an MSDP peer.
Defaults	By default, an MSDP peer is not shut down.
Command Mode	Global configuration mode
Usage Guide	This command shuts down only the TCP connection with an MSDP peer, but does not delete this MSDP peer or configuration of this MSDP peer.

Verification


- Display information about a specified MSDP peer, and check whether the description and peer status meet the requirements.

- ❖ Displaying Information about a Specified MSDP Peer

Command	show ip msdp peer [peer-address]
Parameter Description	N/A
Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	N/A
	<pre> Qtech#show ip msdp peer 20.0.0.1 MSDP PEER 20.0.0.1 (No description), AS unknown Connection status: State: Listen, Resets: 1, Connection source: GigabitEthernet 0/1 (20.0.0.2) Uptime(Downtime): 00:00:25, Message sent/received: 13/19 Input messages discarded: 0 Connection and counters cleared 00:13:25 ago Local Address of connection: 20.0.0.2 MD5 signature protection on MSDP TCP connection: enabled SA Filtering: Input (S,G) Access list filter: None Input (S,G) route map filter: None Input RP Access list filter: None Input RP Route map filter: None Output (S,G) Access list filter: None Output (S,G) Route map filter: None Output RP Access list filter: None Output RP Route map filter: None SA Requests: Input filter: None Peer ttl threshold: 0 SAs learned from this peer: 2, SAs limit: No limit Message counters: SA messages discarded: 0 SA messages in/out: 13/0 SA Requests discarded/in: 0/0 SA Responses out: 0 Data Packets in/out: 6/0 </pre>

Configuration Example

❖ Configuring the Description of an MSDP Peer and Shutting Down the Connection with This Peer

Scenario Figure 8-10	
Configuration Steps	<ul style="list-style-type: none"> ➤ Establish the MSDP peer relationship between device A and device B. ➤ Configure the description "peer-router-B" for the peer 20.0.0.4 on device A. ➤ Wait 60, and shut down the connection with the MSDP peer 20.0.0.4 on device A.
A	<pre>A#configure A(config)# ip msdp peer 20.0.0.4 connect source gi0/1 A(config)# ip msdp description 20.0.0.4 peer router B A(config)# end A# show ip msdp peer 20.0.0.4 A#configure A(config)# ip msdp shutdown 20.0.0.4 A(config)# show ip msdp peer 20.0.0.4</pre>
B	<pre>B# configure B(config)# ip msdp peer 20.0.0.3 connect source gi0/1 B(config)# end</pre>
Verification	<ul style="list-style-type: none"> ➤ Run the show ip msdp peer [peer-address] command to display the brief information of a specified peer, including the description and connection status of this MSDP peer.
A	<pre>A# show ip msdp peer 20.0.0.4</pre>

8.4.7 Modifying Protocol Parameters

Configuration Effect

Manage MSDP peers by adding descriptions to a specified MSDP or reset an MSDP peer.

Notes

- MSDP peers must be created in advance.

Configuration Steps

❖ Configuring the TCP Reconnection Interval of an MSDP Peer

➤ Optional.

- Perform this configuration on the device where the TCP reconnection interval of an MSDP peer needs to be modified.

Command	<code>ip msdp timer interval</code>
Parameter Description	<i>interval</i> : Indicates the TCP reconnection interval. The unit is second. The value ranges from 1 to 60. The default value is 30.
Defaults	By default, the reconnection interval is 30s.
Command Mode	Global configuration mode
Usage Guide	Within the TCP reconnection interval, the MSDP peer on the proactive connection side can initiate at most one TCP connection. In some application scenarios, you can shorten the TCP reconnection interval to accelerate convergence of the MSDP peer relationship.

❖ Configuring the TTL of the Multicast Packet Contained in the SA Message

➤ Optional.

- Perform this configuration on the MSDP device where inter-RP transfer of multicast packets should be restricted.

Command	<code>ip msdp ttl-threshold peer-address ttl-value</code>
Parameter Description	<i>peer-address</i> : Indicates the IP address of an MSDP peer. <i>peer-address ttl-value</i> : Indicates the TTL value. The value ranges from 0 to 255. The default value is 0.
Defaults	By default, the TTL value of the multicast packet contained in the SA message is not restricted.
Command Mode	Global configuration mode
Usage Guide	This command restricts the sending of multicast packet encapsulated in the SA message. A multicast packet is sent to the MSDP peer only when the TTL value in the IP header of the multicast packet is equal to or greater than the preset TTL threshold. If the the TTL value in the IP header of the multicast packet is smaller than the preset TTL threshold, the multicast packet will be removed from the SA message and discarded before the SA message is sent to the MSDP peer. This command affects the sending of multicast packet in the SA message, but does not affect the sending of the multicast source information (S, G) in the SA message.

❖ Configuring the MSDP Peer Capacity Supported by a Device

➤ Optional.

- If the default capacity (64 MSDP peers) is insufficient to support applications, you can modify the capacity on the device.

Command	<code>ip msdp peer-limit peer-limit</code>
----------------	--

Parameter Description	<i>peer-limit</i> : Indicates the maximum number of MSDP peers that can be configured. The value ranges from 1 to 128. The default value is 64.
Defaults	By default, at most 64 peers can be configured.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the maximum number of MSDP peers supported by a device. When configuring this command, if the number of MSDP peers on the device exceeds the value to be configured, a prompt will be displayed, and the configuration fails. The configuration can succeed only after the extra number peers are deleted.

❖ Configuring the SA Cache Capacity Supported by a Device

➤ Optional.

➤ Perform this configuration on a device where the SA cache capacity should be adjusted.


Command	<code>ip msdp global-sa-limit <i>sa-limit</i></code>
Parameter Description	<i>sa-limit</i> : Indicates the maximum capacity of the SA cache supported by the device. The value ranges from 1 to 4,096. The default value is 1,024.
Defaults	By default, the SA cache supports 1,024 SA messages.
Command Mode	Global configuration mode
Usage Guide	This command is used to adjust the SA cache capacity of the device. You are advised to configure this command when the device is being started. If the capacity is increased when MSDP is in service, the adjustment does not affect the SA cache that is originally learned. If the capacity is increased when MSDP is in service, all SA caches that are originally learned from other devices or the SA caches initiated by the local devices must be deleted and re-learned.

Verification

➤ Shut down the connection with an MSDP peer. After the reconnection interval elapses, check whether the MSDP peer is in UP date again.

Configuration Example

❖ Setting the MSDP Peer Reconnection Interval to 20s

Scenario Figure 8-11	
Configuration Steps	<ul style="list-style-type: none"> ➤ Establish the MSDP peer relationship between device A and device B. ➤ On device A, set the MSDP peer reconnection interval to 20s.
A	<pre>A#configure A(config)# ip msdp peer 20.0.0.4 connect source gi0/1</pre>

	<pre>A(config)# ip msdp description 20.0.0.4 peer router B A(config)# end A# show ip msdp peer 20.0.0.4 A#configure A(config)# ip msdp timer 20 A(config)# end</pre>
B	<pre>B# configure B(config)# ip msdp peer 20.0.0.3 connect source gi0/1 B(config)# end</pre>
Verification	<ul style="list-style-type: none"> ➤ On device B, shut down and then immediately reconnect the connection with the MSDP peer. ➤ Check whether the MSDP peer is in UP state within 20s.
A	<pre>A#debug ip msdp timer</pre>
B	<pre>B# configure B(config)# show ip msdp peer 20.0.0.3</pre>

8.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Resets the TCP connection with a specified MSDP peer.	clear ip msdp peer <i>peer-address</i>
Clears the SA cache.	clear ip msdp sa-cache <i>[group-address]</i>
Clears the statistics of MSDP peers.	clear ip msdp statistics <i>[peer-address]</i>

Displaying

Description	Command
Displays the number of sources and number of groups generated by SA messages.	show ip msdp count <i>[as-number]</i>
Displays information about a mesh group.	show ip msdp mesh-group

Description	Command
Displays detailed information about MSDP peers.	show ip msdp peer [<i>peer-address</i>]
Displays information about the MSDP RPF peer corresponding to the specified initiator address.	show ip msdp rpf-peer <i>ip-address</i>
Displays the learned (S, G) information.	show ip msdpsa-cache [<i>group-address</i> <i>source-address</i>] [<i>group-address</i> <i>source-address</i>] [<i>as-number</i>]
Displays the (S, G) information initiated by the local device.	show ip msdpsa-originated
Displays brief information about all MSDP peers.	show ip msdp summary

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs MSDP peers.	debug ip msdp peer

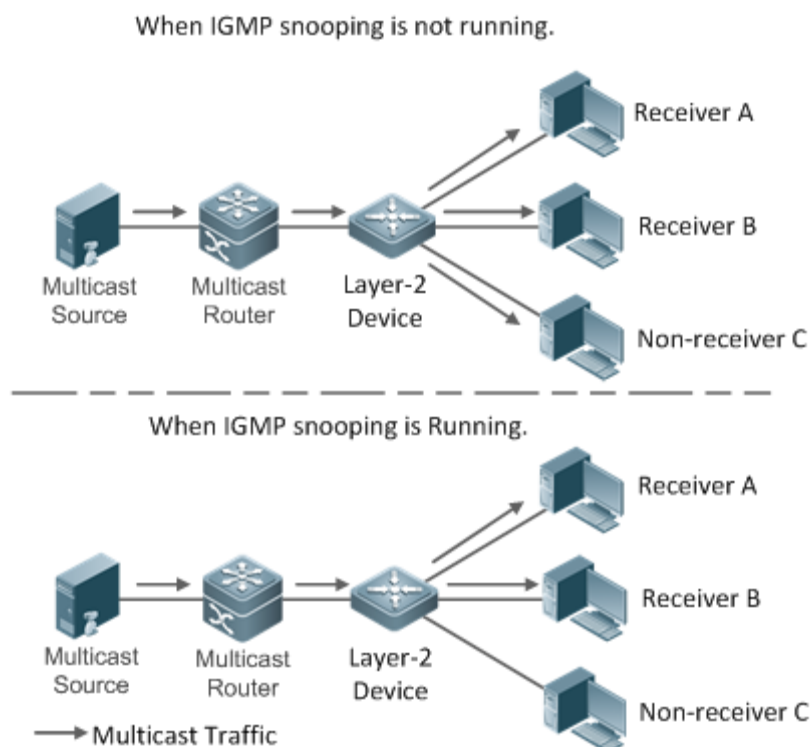
9. CONFIGURING IGMP SNOOPING

9.1 Overview

Internet Group Management Protocol (IGMP) snooping is a mechanism of listening to IP multicast. It is used to manage and control the forwarding of IP multicast traffic within VLANs, realizing Layer-2 multicasting.

As shown in the following figure, when a Layer-2 device is not running IGMP snooping, IP multicast packets are broadcasted within the VLAN; when the Layer-2 device is running IGMP snooping, IP multicast packets are transmitted only to profile members.

Figure 9-1 Networking Topology of IP Multicast Forwarding within the VLAN Before and After IGMP Snooping Is Run on the Layer-2 Device



Protocols and Standards

- RFC4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

9.2 Applications

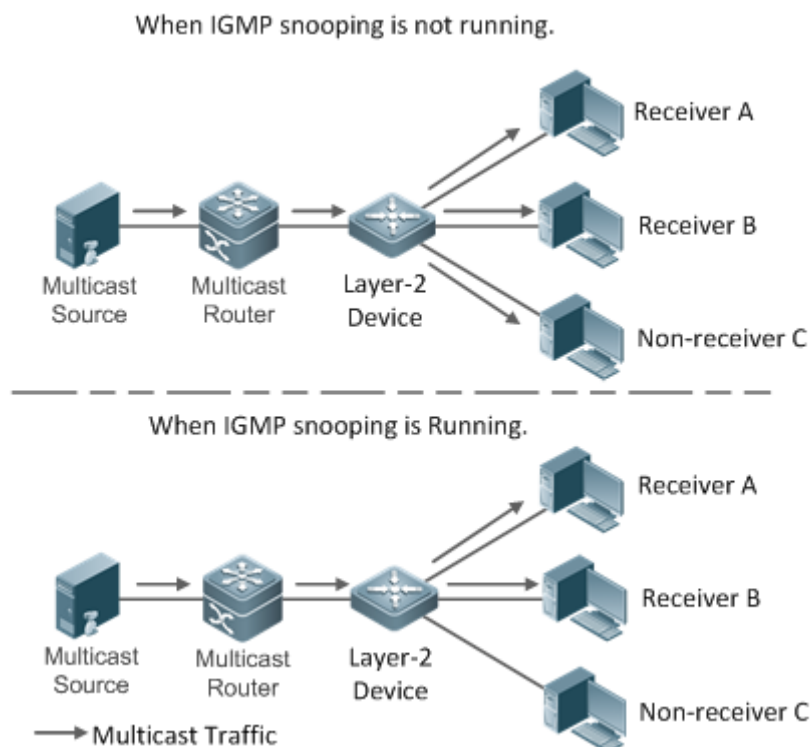
Application	Description
Layer-2 Multicast Control	Enables precise forwarding of Layer-2 multicast packets to avoid flooding at this layer.
Shared Multicast Services (Multicast VLAN)	Multiple users can share the multicast traffic of the same VLAN.
Premium Channels and Preview	Controls the range of multicast addresses that allow user demanding and allows preview for profiles who are inhibited from demanding.

9.2.1 Layer-2 Multicast Control

Scenario

As shown in the following figure, multicast packets are transmitted to users through a Layer-2 switch. When Layer-2 multicast control is not performed, namely, when IGMP snooping is not implemented, multicast packets are flooded to all the users including those who are not expected to receive these packets. After IGMP snooping is implemented, the multicast packets from an IP multicast profile will no longer be broadcast within the VLAN but transmitted to designated receivers.

Figure 9-2 Networking Topology of Implementing Layer-2 Multicast Control (Multicast VLAN)



Deployment

Configure basic IGMP snooping functions.

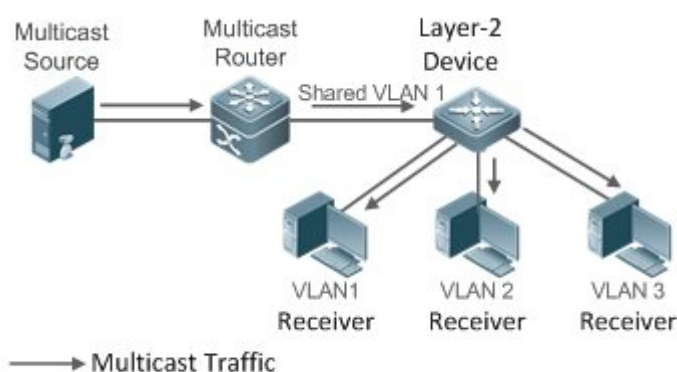
9.2.2 Shared Multicast Services (Multicast VLAN)

Scenario

In Shared VLAN Group Learning (SVGL) mode or IVGL-SVGL mode (IVGL: Independent VLAN Group Learning), a device running IGMP snooping can provide shared multicast services (or multicast VLAN services) to the VLAN users. Typically, this function is used to provide the same video-on-demand (VOD) services to multiple VLAN users.

The following figure shows the operation of a Layer-2 multicast device in SVGL mode of IGMP snooping. The multicast router sends a multicast packet to VLAN 1, and the Layer-2 multicast device automatically transfers the packet to VLAN 1, VLAN 2, and VLAN 3. In this way, the multicast services of VLAN 1 are shared by VLAN 2 and VLAN 3.

Figure 9-3 Networking Topology of Shared Multicast Services (Multicast VLAN)



- If the Layer-2 multicast device operates in IVGL mode, the router must send a packet to each VLAN, which wastes bandwidth and burdens the Layer-2 multicast device.

Deployment

- Configure basic IGMP snooping functions (in SVGL mode or IVGL-SVG mode).

9.2.3 Premium Channels and Preview

Scenario

In VOD application, by limiting the range of the multicast addresses that a user host can access, unpaid users will not be able to watch the premium channels. Thereafter, the preview service is offered to unpaid users before they decide whether to pay for it.

The users can preview a premium channel for a certain period of time (for example 1 minute) after demanding it.

Deployment

- Configure basic IGMP snooping functions (in any working mode).

- Configure the range of multicast addresses that a user can access.
- Enable the preview function for VOD profiles that are denied access.

9.3 Features

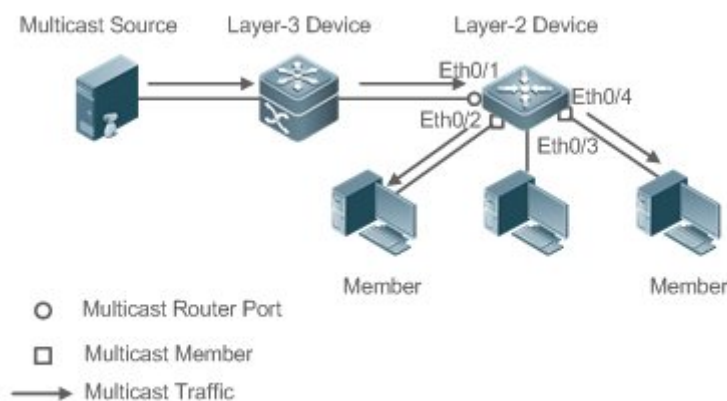
Basic Concepts

❖ Multicast Router Ports and Member Ports

- IGMP snooping is VLAN-based. The ports involved refer to the member ports within the VLAN.

The device running IGMP snooping identifies the ports within the VLAN as a multicast router port or member port so as to manage and control the forwarding of IP multicast traffic within the VLAN. As shown in the following figure, when IGMP snooping is run on a Layer-2 device, multicast traffic enters the multicast router port and exits from the member ports.

Figure 9-4 Networking Topology of Two IGMP Snooping Ports



- Multicast router port: The location of the multicast source is directed by the port on the Layer-2 multicast device which is connected to the multicast router (Layer-3 multicast device): By listening to IGMP packets, the Layer-2 multicast device can automatically detect the multicast router port and maintain the port dynamically. It also allows users to configure a static router port.
- Member port: The port is on a Layer-2 multicast device and is connected to member hosts. It directs the profile members. It is also called the Listener Port. By listening to IGMP packets, the Layer-2 multicast device can automatically detect the member port and maintain the port dynamically. It also allows users to configure a static member port.

❖ IGMP Snooping Forwarding Entry

The device running IGMP snooping forwards IP multicast packets in accordance with the IGMP snooping forwarding entry.

An IGMP snooping forwarding entry includes the following items: source address (S), profile address (G), VLAN ID (VLAN_ID), multicast router port, and member port. It indicates that packets of required features (including S, G, and VLAN_ID) should enter the multicast router port and exit from a member port. An IGMP snooping forwarding entry is identified using a group of S, G, and VLAN_ID.

To display the IGMP snooping forwarding entry, run the **show ip igmp snooping gda-table** command.

```
Qtech# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC //Dynamic member port
  S: STATIC //Static member port
  M: MROUTE //Multicast router port (dynamic or static)
(*, 233.3.6.29, 1): //(S: any; G: 233.3.6.29; VLAN_ID: VLAN 1)
VLAN(1) 3 OPORTS:
  GigabitEthernet 0/3(S)
  GigabitEthernet 0/2(M)
  GigabitEthernet 0/1(D)
(*, 233.3.6.30, 1): //S: any; G: 233.3.6.30; VLAN_ID: VLAN 1)
VLAN(1) 2 OPORTS:
  GigabitEthernet 0/2(M)
  GigabitEthernet 0/1(D)
```

Overview

Feature	Description
Listening to IGMP Packets	Discovers and identifies the router port and member port to establish and maintain the IGMP snooping forwarding entries. :
IGMP Snooping Working Modes	Provides independent or shared multicast services to the user VLAN.
Multicast Security Control Profile	Controls the multicast service scope and load to prevent illegal multicast traffic. Defines the range of multicast addresses that permit or deny user requests for reference of other functions.
Handling QinQ	Sets the forwarding mode of multicast packets on the QinQ interface.
IGMP Querier	On a network without a Layer-3 multicast device, the Layer-2 multicast device acts as an IGMP querier.

9.3.1 Listening to IGMP Packets

A device running IGMP snooping analyzes IGMP packets received, and finds and identifies the router port and member port using these packets, thereby creating and maintaining an IGMP snooping entry.

Working Principle

A device running IGMP snooping can identify and handle the following types of IGMP packets:

❖ Query Packets

-
- An IGMP querier periodically sends General Query packets. When the IGMP querier receives Leave packets, it sends Group-Specific Query packets.
-

When the device running IGMP snooping receives the Query packets, it performs the following operations within the VLAN:

- Forward the IGMP Query packets to all the ports (except the receiving port of these packets).
- If the receiving port is a dynamic router port, reset the aging timer. If the timer expires, the port will no longer be used as the dynamic router port.
- If the receiving port is not a dynamic router port, use it as a dynamic router port and enable the aging timer. If the timer expires, the port will no longer be used as the dynamic router port.
- For general queries, reset the aging timer for all the dynamic member ports. If the timer expires, the port will no longer be used as the dynamic member port for the general group. By default, the maximum response time carried by the IGMP query packets is used as the timeout time of the aging timer. If **ip igmp snooping query-max-response-time** is run, the time displayed is used as the timeout time of the aging timer.
- For designated query packets, reset the aging timer for all the dynamic member ports of the designated profile. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile. By default, the maximum response time carried by the IGMP query packets is used as the timeout time of the aging timer. If **ip igmp snooping query-max-response-time** is run, the time displayed is used as the timeout time of the aging timer.
- If dynamic router port learning is disabled, IGMP snooping will not learn the dynamic router port.

❖ Report Packets

-
- When a member host receives a query, it responds to the query with a Report packet. If a host requests to join a profile, it will also send a report.
 - . For IGMPv3 Report packets, Qtech products only process group information contained in the packets .
-

When the device running IGMP snooping receives the Report packets, it performs the following operations within the VLAN:

- Forward the Report packets from all the router ports. After the **ip igmp snooping suppression enable** command is run in one IGMP query cycle, only the first report received by each profile will be forwarded.
- If the port on which Report packets are received is a dynamic member port, reset the aging timer. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile.
- If the port on which Report packets are received is not a dynamic member port, use it as a dynamic member port and enable the aging timer. If the timer expires, the port will no longer be used as the dynamic member port of the designated profile.

❖ Leave Packets

- If a host requests to leave a profile, it will send a Leave packet.

When the device running IGMP snooping receives the Leave packets, it performs the following operations within the VLAN:

- Forward the leave packets from all the router ports.
- If the port on which leave packets are received is a dynamic member port and the Leave function is enabled, the port will be immediately deleted from the IGMP snooping forwarding entry of the designated profile and will no longer be used as the dynamic member port.
- If the port on which the leave packets are received is a dynamic member port and the Leave function is disabled, the port state should be maintained.

Related Configuration

❖ Configuring a Static Router Port

Run the **ip igmp snooping vlan mrouter interface** command to configure a static router port.

❖ Configuring a Static Member Port

Run the **ip igmp snooping vlan static interface** command to configure a static member port.

❖ Enabling Report Suppression

Report suppression is disabled by default.

Run the **ip igmp snooping suppression enable** command to enable report suppression.

After report suppression is enabled, in one IGMP query cycle, only the first Report packet received by each profile will be forwarded. The source media access control (MAC) address of the forwarded report will be changed to the MAC address of the device.

❖ Enabling Immediate Leave

Immediate leave is disabled by default.

Run the **ip igmp snooping fast-leave enable** command to enable immediate leave.

❖ Enabling Dynamic Router Port Learning

Dynamic router port learning is enabled by default.

Run the **no ip igmp snooping mrouter learn pim-dvmrp** command to disable dynamic router port learning.

Run the **no ip igmp snooping vlan vid mrouter learn pim-dvmrp** command to disable dynamic router port learning for designated VLANs.

❖ Configuring the Aging Time of a Dynamic Router Port

The default aging time is 300s.

When a dynamic router port receives a query packet, the aging timer of the port is enabled or reset; if the aging time is not configured, the maximum response time carried by the query packet is used as the aging time.

Run **ip igmp snooping dyn-mr-aging-time** to configure the aging time of the dynamic router port.

❖ Configuring the Aging Time of a Dynamic Member Port

The default aging time is 260s.

When a dynamic member port receives a query packet, the aging timer of the port is enabled or reset, and the aging time is the maximum response time carried by the query packet.

When a dynamic member port receives a Report packet, the aging timer of the port is enabled or reset, and the aging time is the maximum response time of the dynamic member port.

Run **ip igmp snooping host-aging-time** to configure the aging time of the dynamic member port.

❖ Configuring the Maximum Response Time of a Query Packet

The maximum response time of a query packet is not configured by default and the maximum response time carries by the query packet is used.

Run **ip igmp snooping query-max-response-time** to configure the maximum response time of a query packet.

9.3.2 IGMP Snooping Working Modes

A device running in the three modes (IVGL, SVGL, and IVGL-SVGL) of IGMP snooping can provide independent multicast services or shared multicast services to the user VLAN.

Working Principle

❖ IVGL

In IVGL mode, a device running IGMP snooping can provide independent multicast services to each user VLAN.

Independent multicast services indicate that multicast traffic can be forwarded only within the VLAN it belongs to, and a user host can subscribe to the multicast traffic within the VLAN that the host belongs to.

❖ SVGL

In SVGL mode, a device running IGMP snooping can provide shared multicast services to the user VLAN.

Shared multicast services can be provided only on shared VLANs and sub VLANs and SVGL multicast addresses are used. In a shared VLAN, the multicast traffic within the range of SVGL multicast addresses is forwarded to a sub VLAN, and the user hosts within the sub VLAN subscribe to such multicast traffic from the shared VLAN.

- In a shared VLAN and sub VLAN, shared multicast services will be provided to the multicast traffic within the range of SVGL multicast addresses. Other multicast traffic will be discarded.
- Other VLANs (except shared VLANs and sub VLANs) apply to independent multicast services.

- When the user VLAN is set to a shared VLAN or sub VLAN, shared multicast services are provided; when a user VLAN is set to other VLANs, independent multicast services are provided.

❖ IVGL-SVGL

IVGL-SVGL mode is also called the hybrid mode. In this mode, a device running IGMP snooping can provide both shared and independent multicast services to the user VLAN.

- In a shared VLAN and sub VLAN, multicast services will be provided to the multicast traffic within an SVGL profile. For other multicast traffic, independent multicast services will be provided.
- Other VLANs (except shared VLANs and sub VLANs) apply to independent multicast services.

- When a user VLAN is configured as a shared VLAN or sub VLAN, both public multicast services and independent multicast services are available. When a user VLAN is configured as a VLAN other than shared VLAN and sub VLAN, only the independent multicast services are available.

Related Configuration

❖ Enabling IGMP Snooping and Selecting a Working Mode

IGMP snooping is disabled by default.

Run the **ip igmp snooping ivgl** command to enable IGMP snooping in IVGL mode.

Run the **ip igmp snooping svgl** command to enable IGMP snooping in SVGL mode.

Run the **ip igmp snooping ivgl-svgl** command to enable IGMP snooping in IVGL-SVGL mode.

A working mode must be designated when enabling IGMP snooping, namely, one of the preceding working modes must be selected.

❖ Configuring Shared VLAN

The shared VLAN is VLAN 1 by default.

Run the **ip igmp snooping svgl vlan** command to designate a VLAN as the shared VLAN.

In SVGL mode and IVGL-SVGL mode, only one VLAN can be configured as the shared VLAN.

❖ Configuring Sub VLAN

By default, a sub VLAN is any VLAN except the shared VLAN.

Run the **ip igmp snooping svgl subvlan** command to designate a VLAN as the sub VLAN.

In SVGL mode and IVGL-SVGL mode, the number of sub VLANs is not limited.

❖ Configuring an SVGL Profile

No default setting.

Run the **ip igmp snooping svgl profile *profile_num*** command to configure the address range of an SVGL profile.

In SVGL mode and IVGL-SVGL mode, the SVGL profile range must be configured; otherwise, shared multicast services cannot be provided.

9.3.3 IGMP Security Control

A device running IGMP snooping can control the multicast service scope and load, and effectively prevents illegal multicast traffic.

Working Principle

❖ Configuring the Profile Filtering for User Demanding

By configuring the profile list that a user can access, you can customize the multicast service scope to guarantee the interest of operators and prevent illegal multicast traffic.

To enable this function, you should use a profile to define the range of multicast addresses that a user is allowed to access.

- When the profile is applied on a VLAN, you can define the multicast addresses that a user is allowed to access within the VLAN.
- When the profile is applied on an interface, you can define the multicast addresses that a user is allowed to access under the port.

❖ Multicast Preview

If the service provider wants to allow the users to preview some multicast video traffic that denies the users' access, and stop the multicast video traffic after the preview duration is reached, the user-based multicast preview function should be provided.

The multicast preview function is used together with multicast permission control. For example, in the application of videos, the administrator controls some premium channels by running the **ip igmp profile** command on a port or VLAN. In this way, unsubscribed users will not be able to watch these

channels on demand. If users want to preview the channels before they decide whether to pay for watching or not, the multicast preview function can be enabled, allowing the premium channels to be previewed by unpaid users for a certain period of time (for example 1 minute).

❖ Controlling the Maximum Number of Profiles Allowed for Concurrent Request

If there is too much multicast traffic requested at the same time, the device will be severely burdened. Configuring the maximum number of profiles allowed for concurrent request can guarantee the bandwidth.

- You can limit the number of profiles allowed for concurrent request globally.
- You can also limit the number of profiles allowed for concurrent request on a port.

❖ Controlling the Entry of Multicast Traffic

By running the **ip igmp snooping source-check port** command to enable source port inspection, you can restrict the entry of multicast traffic to prevent illegal traffic.

- When source port inspection is enabled, only the multicast traffic entered from the router port is considered as legal; the traffic from other ports is considered as illegal and will be discarded.
- When source port inspection is disabled, the traffic entered from any port is considered as legal.

❖ Configuring the Source IP Inspection for Multicast Traffic

By enabling source IP inspection, you can restrict the IP address of multicast traffic to prevent illegal traffic.

Source IP inspection includes the inspection of the source IP addresses of specific profiles and of default profiles.

- Inspection of the source IP addresses of default profiles (also called source-check default-server): Specifies the source IP addresses for all the multicast profiles within all VLANs. Only the multicast traffic whose source IP address is the same as the set one is considered as legal.
- Inspection of the source IP addresses of specific profiles (also called limit-ipmc): Specifies the source IP addresses for specific multicast profiles within specific VLANs. Among the multicast traffic received from the specific multicast profiles within the VLANs, only the one with the same source IP address as the set one is considered as legal and will be forwarded by the multicast device; other traffic will be discarded.

Related Configuration

❖ Configuring the Profile Filtering

By default, profiles are not filtered and allow user access.

To filter multicast profiles, run the **ip igmp snooping filter** command in interface configuration mode or global configuration mode.

❖ Enabling Preview

Preview is not enabled by default.

Run the **ip igmp snooping preview** command to enable preview and restrict the range of the profiles permitted for multicast preview.

Run the **ip igmp snooping preview interval** to set the multicast preview duration.

❖ Configuring the Maximum Number of Profiles Allowed for Concurrent Request on a Port

By default, the number of profiles allowed for concurrent request is not limited.

Run the **ip igmp snooping max-groups** command to configure the maximum number of profiles allowed for concurrent request.

❖ Configuring the Maximum Number of Multicast Profiles Allowed Globally

By default, the maximum number of multicast profiles allowed globally is 65,536.

Run the **ip igmp snooping l2-entry-limit** command to configure the maximum number of multicast profiles allowed globally.

❖ Enabling Source Port Inspection

By default, source port inspection is not configured.

Run the **ip igmp snooping source-check port** command to enable source port inspection.

❖ Enabling Source IP Inspection

By default, source IP inspection is disabled.

➤ Run the **ip igmp snooping source-check default-server address** command to enable source IP inspection and specify the default source IP address (applicable to any profile of any VLAN).

➤ (Optional) Run the **ip igmp snooping limit-ipmc vlan vid address group-address server source-address** command to specify a specific source IP address for a specific profile of specific VLAN (applicable to a specific profile of specific VLAN).

First, you must enable source IP inspection to specify default source address, and then a specific source address can be specified for a specific profile of specific VLAN. If a source address is specified for a specific profile of specific VLAN, the multicast traffic of the specific profile will perform inspection for the source address specified by this command. Other multicast traffic will perform inspection for default source addresses.

9.3.4 IGMP Profile

A multicast profile is used to define the range of multicast addresses that permit or deny user demanding request for reference of other functions.

Working Principle

The profile is used to define the range of multicast addresses.

When SVGL mode is enabled, an SVGL profile is used to define the range of SVGL multicast addresses.

When the multicast filter is configured on an interface, a profile is used to define the range of multicast addresses that permit or deny user request under the interface.

When a VLAN filter is configured, a profile is used to define the range of multicast addresses that permit or deny user request under within the VLAN.

When the preview function is enabled, a profile is used to define the range of multicast address allowed for preview.

Related Configuration

❖ Configuring a Profile

Default configuration:

- Create a profile, which is **deny** by default.

Configuration steps:

- Run the **ip igmp profile** *profile-number* command to create a profile.
- Run the **range** *low-address high_address* command to define the range of multicast addresses. Multiple address ranges are configured for each profile.
- (Optional) Run the **permit** or **deny** command to permit or deny user request (**deny** by default). Only one **permit** or **deny** command can be configured for each profile.

9.3.5 IGMP QinQ

Working Principle

On a device with IGMP snooping enabled and dot1q-tunnel (QinQ) port configured, IGMP snooping will handle the IGMP packets received by the QinQ port using the following two approaches:

- Approach 1: Create a multicast entry on the VLAN where IGMP packets are located. The forwarding of IGMP packets on the VLAN where these packets are located is called transparent transmission. For example, presume that IGMP snooping is enabled for a device, Port A is designated as the QinQ port, the default VLAN of this port is VLAN 1, and it allows the passage of VLAN 1 and VLAN 10 packets. When a multicast Query packet is sent by VLAN 10 to Port A, IGMP snooping establishes a multicast entry for VLAN 10 and forwards the multicast Query packet to the router port of VLAN 10.
- Approach 2: Create a multicast entry on the default VLAN of the QinQ port. Encapsulate the multicast packet with the VLAN tag of the default VLAN where the QinQ port is located and forward the packet within the default VLAN. For example, presume that IGMP snooping is enabled for a device, Port A is designated as the QinQ port, the default VLAN of this port is VLAN 1, and it allows the passage of VLAN 1 and VLAN 10 packets. When a multicast Query packet is sent by VLAN 10 to Port A, IGMP snooping establishes a multicast entry for VLAN 1, encapsulates the multicast query packet with the tag of VLAN 1, and forward the packet to

VLAN 1 router port.

Related Configuration

❖ Configuring QinQ

By default, IGMP snooping works in the mode specified in Approach 2.

Run the **ip igmp snooping tunnel** command to implement Approach 1.

9.3.6 IGMP Querier

On a network with a Layer-3 multicast device, the Layer-3 multicast device acts as an IGMP querier. In this case, a Layer-2 device needs only to listen to IGMP packets to establish and maintain the forwarding entry, realizing Layer-2 multicast.

On a network without a Layer-3 multicast device, the Layer-2 multicast device must be configured with the IGMP querier function so that the device can listen to IGMP packets. In this case, a Layer-2 device needs to act as an IGMP querier as well as listen to IGMP packets to establish and maintain the forwarding entry to realize Layer-2 multicast.

Working Principle

A Layer-2 device acts as an IGMP querier to periodically send IGMP Query packets, listen to and maintain the IGMP Report packets replied by a user, and create a Layer-2 multicast forwarding entry. You can adjust relevant parameters of the Query packets sent by the IGMP querier through configuration.

When the device receives a Protocol-Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP) packet, it considers that a multicast router, which will act as an IGMP querier, exists on the network and disables the querier function. In this way, IGMP routing will not be affected.

When the device receives the IGMP Query packets from other devices, it will compete with other devices for the IGMP querier.

❖ Enabling the Querier Function

You can enable the querier for a specific VLAN or all VLANs.

Only when the global querier function is enabled can the queriers for specific VLANs take effect.

❖ Specifying the IGMP Version for a Querier

The version of IGMP used for sending Query packets can be configured as IGMPv1 or IGMPv2.

❖ Configuring the Source IP Address of a Querier

You can configure the source IP address of a query packet sent by the querier based on VLANs.

When the source IP address of the querier is not configured, the querier will not take effect.

❖ Configuring the Query Interval of a Querier

You can configure the intervals for sending global Query packets based on different queriers on different VLANs.

❖ Configuring the Maximum Response Time of a Query Packet

You can configure the maximum response time carried by a Query packet that is sent by a querier. As IGMPv1 does not support the carrying of maximum response time by a Query packet, this configuration does not take effect when the querier is running IGMPv1. You can configure different maximum response time for queriers on different VLANs.

❖ Configuring the Aging Time of a Querier

When other IGMP queriers exist on a network, the existing device will compete with other queriers. If the existing device fails to be elected and is in the non-querier state, the aging timer of a querier will be enabled. After the timer expires, other queriers on the network are considered as expired and the existing device will be resumed as the querier.

Related Configuration

❖ Enabling the Querier Function

By default, the querier function of a device is disabled.

Run the **ip igmp snooping querier** command to enable the global querier function.

Run the **ip igmp snooping vlan num querier** command to enable the querier function for specific VLANs.

❖ Specifying the IGMP Version for a Querier

By default, a querier runs IGMPv2.

Run the **ip igmp snooping querier version** command to configure the global querier version.

Run the **ip igmp snooping vlan querier version** command to specify the querier version for specific VLANs.

❖ Configuring the Source IP Address of a Querier

By default, the source IP address of a querier is 0.

Run the **ip igmp snooping querier address** command to enable global source IP addresses of queriers.

Run the **ip igmp snooping vlan querier address** command to specify the source IP addresses of the queriers on specific VLANs.

❖ Configuring the Query Interval of a Querier

By default, the query interval of a querier is 60s.

Run the **ip igmp snooping querier query-interval** command to enable the global query interval of queriers.

Run **ip igmp snooping vlan querier query-interval** to specify the global query interval of the queriers on specific VLANs.

❖ Configuring the Maximum Response Time of a Query Packet

By default, the maximum response time of a query packet is 10s.

Run the **ip igmp snooping querier max-response-time** command to configure the maximum response time of the query packets sent by global queriers.

Run the **ip igmp snooping vlan querier max-response-time** command to specify the maximum response time of the query packets sent by the queriers on specific VLANs.

❖ Configuring the Aging Time of a Querier

By default, the aging time of a querier is 125s.

Run the **ip igmp snooping querier max-response-time** command to configure the aging time of global queriers.

Run the **ip igmp snooping vlan querier max-response-time** command to configure the aging time of queriers on specific VLANs.

9.4 Configuration

Configuration	Description and Command	
Configuring Basic IGMP Snooping Functions (IVGL Mode)	Any of IVGL mode, SVGL mode, and IVGL-SVGL mode must be selected. It is used to enable IGMP snooping in IVGL mode.	
	ip igmp snooping ivgl	Enables global IGMP snooping in IVGL mode.
	no ip igmp snooping vlan num	Disables IGMP snooping for a VLAN.
Configuring Basic IGMP Snooping Functions (SVGL Mode)	Any of IVGL mode, SVGL mode, and IVGL-SVGL mode must be selected. It is used to enable IGMP snooping in SVGL mode.	
	ip igmp snooping svgl	Enables global IGMP snooping in IVGL mode.
	no ip igmp snooping vlan num	Disables IGMP snooping for a VLAN.
	ip igmp snooping svgl profile profile_num	Configures the SVGL profile.
	ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.
	ip igmp snooping svgl subvlan	Specifies the SVGL sub VLAN.
Configuring Basic IGMP Snooping Functions (IVGL-SVGL Mode)	Any of IVGL mode, SVGL mode, and IVGL-SVGL mode must be selected. It is used to enable IGMP snooping in IVGL-SVGL mode.	

	ip igmp snooping ivgl-svgl	Enables global IGMP snooping in IVGL-SVGL mode.
	no ip igmp snooping vlan <i>num</i>	Disables IGMP snooping for a VLAN.
	ip igmp snooping svgl profile <i>profile_num</i>	Configures the SVGL profile.
	ip igmp snooping svgl vlan	Specifies the SVGL shared VLAN.
	ip igmp snooping svgl subvlan	Specifies the SVGL sub VLAN.
Configuring the Packet Processing	(Optional) It is used to adjust relevant configurations for processing protocol packets.	
	ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i>	Configures a static router port.
	p igmp snooping vlan <i>vid</i> static group-address interface <i>interface-type</i> <i>interface-number</i>	Configures a static member port.
	ip igmp snooping vlan <i>vlan-id</i> mrouter learn pim-dvmrp	Enables dynamic router port learning.
	ip igmp snooping dyn-mr-aging-time <i>time</i>	Configures the aging time of a dynamic router port.
	ip igmp snooping host-aging-time <i>time</i>	Configures the aging time of a dynamic member port.
	ip igmp snooping fast-leave enable	Enables the immediate-leave function for a dynamic member port.
	ip igmp snooping query-max-response-time <i>time</i>	Configures the maximum response time of an IGMP query packet.
	ip igmp snooping suppression enable	Enables IGMP Report packet suppression.
Configuring IGMP Security Control	(Optional) It used to guarantee the security when a user requests a multicast profile.	
	ip igmp snooping filter <i>profile-number</i>	Configures the profile filtering for user access.
	ip igmp snooping vlan <i>num</i> filter <i>profile-number</i>	Configures the per-VLAN profile filtering for user access.
	ip igmp snooping l2-entry-limit <i>number</i>	Configures the maximum number of profiles globally for user access.
	ip igmp snooping max-groups <i>number</i>	Configures the maximum number of dynamic profiles for user access.
ip igmp snooping source-check port	Enables source IP inspection, which ensures the multicast traffic from the router port is legal.	

	ip igmp snooping source-check default-server address	Enables source IP inspection. The multicast traffic whose source IP address matches the specified source IP address is considered as legal traffic.
	ip igmp snooping limit-ipmc vlan vid address group-address server source-address	Specifies a VLAN. In the multicast traffic of multicast addresses, the one whose source IP address matches the specified source IP address is considered as legal traffic.
	ip igmp snooping preview profile-number	Enables the preview function for a specified profile.
	ip igmp snooping preview interval num	Configures the preview duration.
Configuring an IGMP Profile	(Optional) It is used to define the range of multicast addresses that permits or denies the access of a user host.	
	ip igmp profile profile-number	Creates a profile.
	range low-address high_address	Configures the profile range.
	permit	Permits the access of a user host.
	deny	Denies the access of a user host.
Configuring IGMP QinQ	(Optional) It is used to configure QinQ interface to forward multicast packets using the VLAN identifier (VID) carried by packets.	
	ip igmp snooping tunnel	Configures QinQ to transmit IGMP packets transparently.
Configuring an IGMP Querier	(Optional) It is used to enable IGMP querier function on a network without a Layer-3 multicast device.	
	ip igmp snooping querier	Enables global querier function.
	ip igmp snooping vlan num querier	Enables the querier for a VLAN.
	ip igmp snooping querier version num	Specifies the IGMP version for queriers globally.
	ip igmp snooping vlan num querier version num	Specifies the IGMP version for a querier of a VLAN.
	ip igmp snooping querier address a.b.c.d	Configures the source IP address of queriers globally.
	ip igmp snooping vlan num querier address a.b.c.d	Configures the source IP address for a querier of a VLAN.
	ip igmp snooping querier query-interval num	Configures the query interval of queriers globally.
ip igmp snooping vlan num querier query-interval num	Configures the query interval for a querier of a VLAN.	

	ip igmp snooping querier max-response-time num	Configures the maximum response time for query packets globally.
	ip igmp snooping vlan num querier max-response-time num	Configures the maximum response time of query packets for a VLAN.
	ip igmp snooping querier timer expiry num	Configures the aging timer for queriers globally.
	ip igmp snooping vlan num querier timer expiry num	Configures the aging timer for a querier of a VLAN.

9.4.1 Configuring Basic IGMP Snooping Functions (IVGL Mode)

Configuration Effect

- Enable IGMP snooping to realize Layer-2 multicast.
- Provide independent multicast services to each VLAN.

Notes

- IP multicast cannot be realized in SVGL mode. If IP multicast must be used, select the IVGL mode.

Configuration Steps

- ❖ Enabling Global IGMP Snooping in IVGL Mode

Mandatory.

After IGMP snooping is enabled globally, this function will be enabled for all VLANs.

If not specified, it is advised to run global IGMP snooping on all the devices connected user hosts.

- ❖ Disabling IGMP Snooping for a VLAN

(Optional) You can use this function if you wish to disable IGMP snooping on specified VLANs.

Only when global IGMP snooping is enabled can it be disabled on specified VLANs.

In IVGL mode, each VLAN can enjoy independent multicast services. Disabling any VLAN multicast services will not interfere in the services provided to the others.

Verification

- Run the **show ip igmp snooping gda-table** command to display the IGMP snooping forwarding table and verify that the member ports include only those connecting member hosts.
- Run the **show ip igmp snooping** command to display the basic IGMP snooping information and verify that IGMP snooping is working in IVGL mode.

Related Commands

- ❖ Enabling Global IGMP Snooping in IVGL Mode

Command	<code>ip igmp snooping ivgl</code>
---------	------------------------------------

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After this command is executed, IGMP snooping will be run on all VLANs. By default, IGMP snooping is disabled.

❖ Disabling IGMP Snooping for a VLAN

Command	<code>no ip igmp snooping vlan num</code>
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Only when global IGMP snooping is enabled can it be disabled on specified VLANs. In IVGL mode, you can disable IGMP snooping on any VLAN.

❖ Displaying the IGMP Snooping Entry

Command	<code>show ip igmp snooping gda-table</code>
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	This command is used to verify that the ports include only those connecting member hosts.

❖ Displaying the IGMP Snooping Working Mode

Command	<code>show ip igmp snooping</code>
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in IVGL mode, the following information is displayed: IGMP Snooping running mode: IVGL

Configuration Example

❖ Providing Layer-2 Multicast Services for the Subnet Hosts

<p>Scenario Figure 9-5</p>	
	<p>A is the multicast router and is connected directly to the multicast source. B is the Layer-2 device and is connected directly to the user host. Receiver 1, Receiver 2, and Receiver 3 belong to VLAN 1.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure the IP address and VLAN. ➤ Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ➤ Enable IGMP snooping on B and select IVGL mode.
<p>A</p>	<pre>A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit</pre>
<p>B</p>	<pre>B# configure terminal B(config)# ip igmp snooping ivgl</pre>
<p>Verification</p>	<p>Send packets from the source (10.1.1.1) to G (229.1.1.1) to add Receiver 1 to G.</p> <ul style="list-style-type: none"> ➤ Confirm that the packets (10.1.1.1 and 229.1.1.1) are received by Receiver 1. ➤ Display the IGMP snooping forwarding entry on B and ensure that the port (10.1.1.1, 229.1.1.1, 1) includes only Fa0/2. ➤ Check whether the IGMP snooping working mode is IVGL.
<p>B</p>	<pre>B# show ip igmp snooping gda-table</pre>

Multicast Switching Cache Table

D: DYNAMIC

S: STATIC

M: MROUTE

(* ,224.1.1.1, 1):

VLAN(1) 2 OPORTS:

FastEthernet 0/1(M)

FastEthernet 0/2(D)

B# show ip igmp snooping

IGMP Snooping running mode: IVGL

IGMP Snooping L2-entry-limit: 65536

Source port check: Disable

Source ip check: Disable

IGMP Fast-Leave: Disable

IGMP Report suppress: Disable

IGMP Global Querier: Disable

IGMP Preview: Disable

IGMP Tunnel: Disable

IGMP Preview group aging time : 60(Seconds)

Dynamic Mroute Aging Time : 300(Seconds)

Dynamic Host Aging Time : 260(Seconds)

vlan 1

IGMP Snooping state: Enable

Multicast router learning mode: pim-dvmrp

IGMP Fast-Leave: Disabled

IGMP VLAN querier: Disable

IGMP VLAN Mode: STATIC

Common Errors

- The working mode of IGMP snooping is improper.

9.4.2 Configuring Basic IGMP Snooping Functions (SVGL Mode)

Configuration Effect

- Enable IGMP snooping and select SVGL mode to realize Layer-2 multicast.
- Share the VLAN multicast services.

Configuration Steps

- ❖ Enabling Global IGMP Snooping in SVGL Mode

Mandatory.

Enable global IGMP snooping in SVGL mode.

Configure the range of associated SVGL profiles.

- ❖ Specifying the SVGL Shared VLAN

(Optional) By default, VLAN 1 is used as the shared VLAN. You can adjust this configuration for other options.

- ❖ Specifying the SVGL Sub VLAN

(Optional) By default, all the VLANs are used as the sub VLANs of SVGL and can share the multicast services of the shared VLAN. You can adjust this configuration for other options.

Verification

- Run the **show ip igmp snooping** command to display the basic IGMP snooping information and verify that IGMP snooping is working in SVGL mode.
- Run the **show ip igmp snooping gda-table** command to check whether inter-VLAN multicast entries are properly formed.

Related Commands

- ❖ Enabling Global IGMP Snooping in SVGL Mode

Command	ip igmp snooping svgl
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, IGMP snooping is disabled. After the SVGL mode is selected, the range of profiles within SVGL multicast addresses needs to be associated.

❖ Configuring the SVGL profile

Command	ip igmp snooping svgl profile <i>profile_num</i>
Parameter Description	<i>profile_num</i> : Configures SVGL to associate a profile.
Command Mode	Global configuration mode
Usage Guide	By default, no profile is associated with SVGL.

❖ Specifying the SVGL Shared VLAN

Command	ip igmp snooping svgl vlan <i>vid</i>
Parameter Description	<i>vid</i> : Indicates a VLAN.
Command Mode	Interface configuration mode
Usage Guide	By default, VLAN 1 is used as the shared VLAN.

❖ Specifying the SVGL Sub VLAN

Command	ip igmp snooping svgl subvlan <i>vid-range</i>
Parameter Description	<i>vid-range</i> : Indicates VLAN ID or the range of VLAN IDs.
Command Mode	Interface configuration mode
Usage Guide	By default, all the VLANs except the shared VLAN are used as sub VLANs.

❖ Displaying the IGMP Snooping Working Mode

Command	show ip igmp snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in SVGL mode, the following information is displayed: <pre>IGMP Snooping running mode: SVGL</pre>

Configuration Example

❖ Enabling SVGL on the Access Device

<p>Scenario Figure 9-6</p>	
	<p>A is the multicast router and is connected directly to the multicast source. B is the Layer-2 device and is connected directly to the user host. Receiver 1 is connected to VLAN 2, Receiver 2 is connected to VLAN 3, and Receiver 3 is connected to VLAN 4.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure the IP address and VLAN. (Omitted) ➤ Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ➤ Enable IGMP snooping on B and select SVGL mode. ➤ Configure the range of associated SVGL multicast addresses on B.
<p>A</p>	<pre>A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit</pre>
<p>B</p>	<pre>B# configure terminal B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#range 224.1.1.1 238.1.1.1 B(config-profile)#exit B(config)#ip igmp snooping svgl</pre>

	<code>B(config)#ip igmp snooping svgl profile 1</code>
Verification	<p>Send packets from the source (10.1.1.1) to G (229.1.1.1) and add Receiver 1, Receiver 2 and Receiver 3 to G.</p> <ul style="list-style-type: none"> ➤ Confirm that the packets (10.1.1.1 and 224.1.1.1) are received by Receiver 1, Receiver 2, and Receiver 3. ➤ Display the IGMP snooping forwarding entry on B and ensure that the ports (*, 224.1.1.1, 1) include Gi0/2, Gi0/3, and Gi0/4. ➤ Check whether the IGMP snooping working mode is SVGL.
B	<pre> B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*,224.1.1.1, 1): VLAN(2) 1 OPORTS: GigabitEthernet 0/2(D) VLAN(3) 1 OPORTS: GigabitEthernet 0/3(D) VLAN(4) 1 OPORTS: GigabitEthernet 0/4(D) B# show ip igmp snooping IGMP Snooping running mode: SVGL IGMP Snooping L2-entry-limit: 65536 SVGL vlan: 1 SVGL profile number: 1 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) </pre>

Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)

Common Errors

- The SVGL profile is not configured.
- The sent multicast traffic is not within the SVGL profile.

9.4.3 Configuring Basic IGMP Snooping Functions (IVGL-SVGL Mode)

Configuration Effect

- Enable IGMP snooping and select IVGL-SVGL mode to realize Layer-2 multicast.
- The SVGL profiles can share the multicast services.
- The non-SVGL profiles run in IVGL mode.

Configuration Steps

- ❖ Enabling Global IGMP Snooping in IVGL-SVGL Mode

Mandatory.

Enable global IGMP snooping in IVGL-SVGL mode.

Configure the range of associated SVGL profiles.

- ❖ Specifying the SVGL Shared VLAN

(Optional) By default, VLAN 1 is used as the shared VLAN. You can adjust this configuration for other options.

- ❖ Specifying the SVGL Sub VLAN

(Optional) By default, all the VLANs are used as the sub VLANs of SVGL and can share the multicast services of the shared VLAN. You can adjust this configuration for other options.

Verification

- Run the **show ip igmp snooping** command to display the basic IGMP snooping information and verify that IGMP snooping is working in IVGL-SVGL mode.
- Run the **show ip igmp snooping gda-table** command to check whether inter-VLAN multicast entries are properly formed for the SVGL profiles.
- Run the **show ip igmp snooping gda-table** command to check whether intra-VLAN multicast entries are properly formed for the SVGL profiles.

Related Commands

- ❖ Enabling Global IGMP Snooping in IVGL-SVGL Mode

Command	ip igmp snooping ivgl-svgl
---------	----------------------------

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, IGMP snooping is disabled. After the IVGL-SVGL mode is selected, the SVGL profiles needs to be associated.

❖ Configuring the SVGL Profile

Command	ip igmp snooping svgl profile <i>profile_num</i>
Parameter Description	<i>profile_num</i> : Configures SVGL to associate a profile.
Command Mode	Global configuration mode
Usage Guide	By default, no profile is associated with SVGL.

❖ Specifying the SVGL Shared VLAN

Command	ip igmp snooping svgl vlan <i>vid</i>
Parameter Description	<i>vid</i> : Indicates a VLAN.
Command Mode	Interface configuration mode
Usage Guide	By default, VLAN 1 is used as the shared VLAN.

❖ Specifying the SVGL Sub VLAN

Command	ip igmp snooping svgl subvlan <i>vid-range</i>
Parameter Description	<i>vid-range</i> : Indicates VLAN ID or the range of VLAN IDs.
Command Mode	Interface configuration mode
Usage Guide	By default, all the VLANs except the shared VLAN are used as sub VLANs.

❖ Displaying the IGMP Snooping Working Mode

Command	show ip igmp snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in SVGL mode, the following information is displayed: IGMP Snooping running mode: SVGL

❖ Displaying the IGMP Snooping Working Mode

Command	show ip igmp snooping
----------------	------------------------------

Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If a device is running in IVGL-SVGL mode, the following information is displayed: <div style="background-color: #e0e0e0; padding: 2px;">IGMP Snooping running mode: IVGL-SVGL</div>

Configuration Example

❖ Enabling IVGL-SVGL on the Access Device

<p>Scenario Figure 9-7</p>	
	<p>A is the multicast router and is connected directly to multicast Source 1. B is a Layer-2 device and is connected directly to the user host and multicast Source 2. Receiver 1 is connected to VLAN 2, Receiver 2 is connected to VLAN 3, and Receiver 3 is connected to VLAN 4.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure the IP address and VLAN. ➤ Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ➤ Enable IGMP snooping on B and select IVGL-SVGL mode. ➤ Configure the range of associated SVGL multicast addresses on B.
<p>A</p>	<pre>A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1</pre>

	<pre>A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit</pre>
B	<pre>B# configure terminal B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#range 224.1.1.1 238.1.1.1 B(config-profile)#exit B(config)#ip igmp snooping ivgl-svgl B(config)#ip igmp snooping svgl profile 1</pre>
Verification	<p>Send packets from Source 1 (10.1.1.1) to G (224.1.1.1) and add Receiver 1, Receiver 2 and Receiver 3 to G.</p> <p>Send packets from Source 2 (192.168.2.1) to the destination (239.1.1.1) and add Receiver 1 239.1.1.1.</p> <ul style="list-style-type: none"> ➤ Confirm that the packets (10.1.1.1 and 224.1.1.1) are received by Receiver 1, Receiver 2, and Receiver 3. ➤ Check that packets (192.168.2.1 and 239.1.1.1) can be received by Receiver 1. ➤ Display the IGMP snooping forwarding entry on B and ensure that the ports (*, 224.1.1.1, 1) include Gi0/2, Gi0/3, and Gi0/4, and the port (*, 239.1.1.1, 1) is Gi0/2. ➤ Check whether the IGMP snooping working mode is IVGL-SVGL.
B	<pre>B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*,224.1.1.1, 1): VLAN(2) 1 OPORTS: GigabitEthernet 0/2(D) VLAN(3) 1 OPORTS: GigabitEthernet 0/3(D) VLAN(4) 1 OPORTS: GigabitEthernet 0/4(D) (*,239.1.1.1, 2): VLAN(2) 1 OPORTS:</pre>

GigabitEthernet 0/2(D)
<pre>B# show ip igmp snooping IGMP Snooping running mode: IVGL-SVGL IGMP Snooping L2-entry-limit: 65536 SVGL vlan: 1 SVGL profile number: 0 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)</pre>

Common Errors

- The SVGL profile is not configured.
- The sent multicast traffic is not within the SVGL profile.
- The IVGL multicast traffic cannot be forwarded within the SVGL profile.

9.4.4 Configuring the Packet Processing

Configuration Effect

- Configure specified ports as the static router ports to receive the multicast traffic from all profiles.
- Configure specified ports as the static member ports to receive the multicast traffic from specified profiles
- Enable Report packets suppression to forward only the first Report packet from a specified VLAN or profile to the router port within a query interval, and the following Report packets will

not be forwarded to the router port, thereby reducing the quantity of packets on the network.

- Configure the immediate-leave function to delete a port from the entry of member ports when a leave packet is received by the port.
- Disable dynamic router port learning to disable the learning of any router port.
- Based on network load and configuration of a multicast device, you can adjust the aging time of a router port and member port as well as the maximum response time of a query packet.

Notes

- Only when basic IGMP snooping is configured can relevant configurations take effect.

Configuration Steps

❖ Configuring a Static Router Port

- Optional.
- You can perform this configuration if you want to specify a static port to receive all the multicast traffic within the VLAN.

❖ Configuring a Static Member Port

- Optional.
- You can perform this configuration if you want to specify a static port to receive specific multicast traffic within the VLAN.

❖ Enabling Report Packet Suppression

- Optional.
- When there are numerous receivers to receive the packets from the same multicast profile, you can enable Report packets suppression to suppress the number of Report packets to be sent.

❖ Enabling the Immediate-Leave Function

- Optional.
- When there is only one receiver on a port, you can enable Leave to speed up the convergence of protocol upon leave.

❖ Disabling Dynamic Router Port Learning

- Optional.
- This function is used when multicast traffic needs to be forwarded only within the Layer-2 topology but not to a Layer-3 router.

❖ Configuring the Aging Time of a Dynamic Router Port

- Optional.
- You can configure the aging time based on network load.

❖ Configuring the Aging Time of a Dynamic Member Port

- Optional.

- You can configure the aging time based on the interval for sending IGMP query packets by the connected multicast router. Typically, the aging time is calculated as follows: Interval for sending IGMP query packets x 2 + Maximum response time of IGMP packets
- ❖ Configuring the Maximum Response Time of a Query Packet
- Optional.
- You can configure the aging time based on network load.

Verification

- Run the **show ip igmp snooping mrouter** command to check whether the configured static router port has an "S" in the displayed configuration information.
- Run the **show ip igmp snooping gda** command to check whether the configured static member port is marked with an S.
- Run the **show ip igmp snooping** command to check whether Report packets suppression, immediate leave, router port learning, router port aging time, member port aging time, and the maximum response time of the Query packet take effect.

Related Commands

- ❖ Configuring a Static Router Port

Command	ip igmp snooping vlan <i>vid</i> mrouter interface <i>interface-type interface-number</i>
Parameter	<i>vid</i> : Indicates a VLAN. The value ranges from 1 to 4,094.
Description	<i>interface-type interface-number</i> : Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	In SVGL mode, if a sub VLAN is not configured, only the configurations for the static router port within the shared VLAN can take effect, and the others can be configured but cannot take effect. If a sub VLAN is configured, only the configurations for the static router port within the shared VLAN or a non-sub VLAN can take effect, and the others can be configured but cannot take effect. In IVGL-SVGL mode, if a sub VLAN is not configured, the configurations for the static router ports within all the VLANs can take effect; if a sub VLAN is configured, only the configurations for the static router port within the shared VLAN or a non-sub VLAN can take effect, and the others can be configured but cannot take effect. In IVGL mode, the configurations for the static router ports within all the VLANs can take effect.

- ❖ Configuring a Static Member Port

Command	ip igmp snooping vlan <i>vid</i> static <i>group-address</i> interface <i>interface-type interface-number</i>
Parameter	<i>vid</i> : Indicates a VLAN. The value ranges from 1 to 4,094.
Description	<i>group-address</i> : Indicates a profile address. <i>interface-type interface-number</i> : Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	By default, no static member port is configured.

❖ Enabling Report Packet Suppression

Command	ip igmp snooping suppression enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When Report packets suppression is enabled, only the first Report packet from a specified VLAN or profile is forwarded to the router port within a Query interval, and the following Report packets will not be forwarded to the router port, thereby reducing the quantity of packets on the network. Only the IGMPv1 and IGMPv2 Report packets can be suppressed, and the IGMPv3 Report packets cannot be suppressed.

❖ Enabling the Immediate-Leave Function

Command	ip igmp snooping fast-leave enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When this function is enabled, a port will be deleted from the entry of the member port when the port receives a leave packet. After that, the packets will no longer be forwarded to this port when it receives the query packets of specified profiles. Leave packets include the IGMPv2 Leave packets as well as the IGMPv3 Report packets that include types but carry no source address. The immediate-leave function applies only to the scenario where only one host is connected to a device port. It is used to conserve bandwidth and resources.

❖ Enabling Dynamic Router Port Learning

Command	ip igmp snooping [vlan vid] mrouter learn pim-dvmrp
Parameter Description	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	A router port is the port that is connected directly to a multicast device running IGMP snooping and a multicast neighbor device running multicast routing protocol. By default, dynamic router port learning is enabled and the device automatically listens to IGMP Query packets, DVMRP packets, and PIM Hello packets.

❖ Configuring the Aging Time of a Dynamic Router Port

Command	ip igmp snooping dyn-mr-aging-time seconds
Parameter Description	seconds: Indicates the aging time of a dynamic router port in the unit of seconds. The value ranges from 1 to 3,600.
Command Mode	Global configuration mode

Usage Guide	<p>If a dynamic router port does not receive an IGMP general query packet or a PIM Hello packet before the aging timer expires, the device will delete this port from the router port entry.</p> <p>When dynamic router port learning is enabled, you can run this command to adjust the aging time of the dynamic router port. If the aging time is too short, the multicast device may frequently add or delete a router port.</p>
--------------------	--

❖ Configuring the Aging Time of a Dynamic Member Port

Command	ip igmp snooping host-aging-time <i>seconds</i>
Parameter Description	<i>seconds</i> : Indicates the aging time.
Command Mode	Global configuration mode
Usage Guide	<p>The aging time of a dynamic member port indicates the time when a device port receives the IGMP join packet sent from host for subscribing to an IP multicast profile.</p> <p>When the IGMP join packet is received, the aging time of the dynamic member port will be reset. The value of the timer time is host-aging-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port. After the aging time is configured, the aging time of following received IGMP join packets will be host-aging-time. This configuration takes effect after the next IGMP join packet is received, and the timer of the port in use will not be refreshed.</p>

❖ Configuring the Maximum Response Time of a Query Packet

Command	ip igmp snooping query-max-response-time <i>seconds</i>
Parameter Description	<i>seconds</i> : Indicates the maximum response time.
Command Mode	Global configuration mode
Usage Guide	<p>When an IGMP general Query packet is received, the multicast device will reset the aging time of all the dynamic member ports, which is query-max-response-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port.</p> <p>When an IGMP profile-specific Query packet is received, the multicast device will reset the aging time of all the dynamic member ports of the specific profile, which is query-max-response-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port.</p> <p>This configuration takes effect after the next Query packet is received, and the timer in use will not be refreshed. The timer of an IGMPv3 profile-specific Query packet is not refreshed.</p>

❖ Displaying Router Ports

Command	show ip igmp snooping mroute
----------------	-------------------------------------

Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If the router port is successfully configured, an "S" will be displayed in the port information.</p> <pre>Qtech(config)#show ip igmp snooping mrouter Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/1(S)</pre>

❖ Displaying the Information of Dynamic Router Port Learning

Command	show ip igmp snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>Run the show ip igmp snooping command to display the aging time and learning status of the dynamic router port.</p> <pre>Dynamic Mroute Aging Time : 300(Seconds) Multicast router learning mode: pim-dvmrp</pre>

❖ Displaying the Information of a Member Port

Command	show ip igmp snooping gda-table
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If the member port is successfully configured, an "S" will be displayed in the port information.</p> <pre>Qtech(config)#show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*, 224.1.1.1, 1):</pre>

	VLAN(1) 1 OPORTS: GigabitEthernet 0/1(S)
--	---

❖ Displaying Other Parameters

Command	show ip igmp snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Run the show ip igmp snooping command to display the aging time of the router port, aging time of the dynamic member port, response time of the query packet, and Report packets suppression, and immediate leave. <pre>IGMP Fast-Leave: Enable IGMP Report suppress: Enable Query Max Response Time: 20(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)</pre>

Configuration Example

❖ Configuring a Static Router Port and Static Member Port

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic IGMP snooping functions. ➤ Configure a static router port and static member port.
	<pre>Qtech# configure terminal Qtech(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet 0/0 Qtech(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/0 Qtech(config)# end</pre>
Verification	Run the show ip igmp snooping mrouter and show ip igmp snooping gda-table commands to check whether the configuration takes effect.
	<pre>Qtech#show ip igmp snooping mrouter Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/0(S)</pre>

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure basic IGMP snooping functions. ➤ Configure a static router port and static member port.
	<pre>Qtech# configure terminal Qtech(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet 0/0 Qtech(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/0 Qtech(config)# end</pre>
Verification	<p>Run the show ip igmp snooping mrouter and show ip igmp snooping gda-table commands to check whether the configuration takes effect.</p>
	<pre>Qtech#show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*, 224.1.1.1, 1): VLAN(1) 1 OPORTS: GigabitEthernet 0/0(SM)</pre>

❖ Enabling Report Packet Suppression

<p>Scenario Figure 9-8</p>	
	<p>A is the multicast router and is connected directly to multicast Source 1. B is a Layer-2 device and is connected directly to the user host and multicast Source 2. Receiver 1, Receiver 2, and Receiver 3 are connected to VLAN 1.</p>

Configuration Steps	<ul style="list-style-type: none"> ➤ Configure the IP address and VLAN. (Omitted) ➤ Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ➤ Enable IGMP snooping on B and select IVGL mode. ➤ Enable Report packets suppression on B.
A	<pre>A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit</pre>
B	<pre>B# configure terminal B(config)# ip igmp snooping ivgl B(config)# ip igmp snooping suppression enable</pre>
Verification	<p>Check whether Receiver 1 and Receiver 2 are added to profile 239.1.1.1, and only the IGMP Report packets of profile 239.1.1.1 are forwarded from interface Gi0/1 of B.</p>
B	<pre>B# show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)</pre>

❖ Configuring Other Parameters

<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure basic IGMP snooping functions. ➤ Enable Immediate-leave function. ➤ Disable router port learning. ➤ Configure the aging time of a router port. ➤ Configuring the aging time of a member port. ➤ Configure the response time of a Query packet.
	<pre>Qtech# configure terminal Qtech(config)# ip igmp snooping fast-leave enable Qtech(config)# no ip igmp snooping mrouter learn pim-dvmrp Qtech(config)#ip igmp snooping dyn-mr-aging-time 200 Qtech(config)#ip igmp snooping host-aging-time 100 Qtech(config)#ip igmp snooping query-max-response-time 60 Qtech(config)# end</pre>
<p>Verification</p>	<p>Run the show ip igmp snooping command to check whether the configuration is successful.</p>
	<pre>Qtech#show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Enable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable Query Max Response Time: 60(Seconds) IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 200(Seconds) Dynamic Host Aging Time : 100(Seconds)</pre>

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.

9.4.5 Configuring IGMP Security Control

Configuration Effect

- Configure the range of multicast addresses that a user can access.
- Configure to allow a user from an unauthorized profile to preview a multicast channel.
- Configure the number of multicast addresses that a user can access.
- Configure to limit a user to receive only the multicast traffic from a router port to prevent illegal multicast traffic sent by the end user.
- Configure to limit a user to receive only the multicast traffic from designated source IP addresses to prevent illegal multicast traffic.

Notes

- Basic IGMP snooping functions must be configured.

Configuration Steps

❖ Configuring the Profile Filtering

- Optional.
- If you want to limit the profile packets to be received by a port, you can configure the profile filtering on the port.
- If you want to limit the multicast packets to be received by a VLAN, you can configure the per-VLAN profile filtering.

❖ Enabling Multicast Preview

- Optional.
- You can enable multicast preview for a user from an unauthorized profile.

❖ Configuring the Maximum Number of Profiles

- Optional.
- If you want to limit the number of multicast profiles that a port is allowed to receive, you can configure the maximum number of multicast profiles allowed for this port.
- If you want to limit the number of multicast profiles that global ports are allowed to receive, you can configure the maximum number of multicast profiles allowed for these ports.

❖ Configuring Source Port Inspection

- Optional.
- You can perform this configuration if you want to allow a port to receive only the multicast traffic from the router port.

❖ Configuring Source IP Inspection

- Optional.
- You can perform this configuration to specify the source IP address for all the multicast profiles of all VLANs. Only the multicast traffic whose source IP address is the same as the set one is considered as legal.
- You can also specify the source IP addresses for specific multicast profiles within specific VLANs.

Among the multicast traffic received from the specific multicast profiles within the VLANs, only the one with the same source IP address as the set one is considered as legal and will be forwarded by the multicast device; other traffic will be discarded.

Verification

- Run the **show ip igmp snooping interfaces** command to display the profile filtering and the maximum number of multicast profiles for a port.
- Run the **show ip igmp snooping vlan** command to display the per-VLAN profile filtering.
- Run the **show ip igmp snooping** command to check whether the maximum number of global multicast profiles, preview function, source port inspection, and source IP address inspection take effect.

Related Commands

❖ Configuring the Profile Filtering

Command	ip igmp snooping filter <i>profile-number</i>
Parameter Description	<i>profile-number</i> : Indicates a profile number.
Command Mode	Interface configuration mode
Usage Guide	N/A

❖ Configuring the Per-VLAN Profile Filtering

Command	ip igmp snooping vlan <i>vid filter profile-number</i>
Parameter Description	<i>vid</i> : Indicates a VLAN. The value ranges from 1 to 4,094. <i>profile-number</i> : Indicates a profile number.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring the Maximum Number of Profiles on a Port

Command	ip igmp snooping max-groups <i>number</i>
Parameter Description	<i>number</i> : Indicates the maximum number of multicast profiles.
Command Mode	Interface configuration mode
Usage Guide	This value indicates only the number of dynamic multicast profiles, and the number of static profiles is not included. The counter of multicast profiles is based on the VLAN that the port belongs to. For example, if a port belongs to three VLANs, and all three of them receive a request packet from multicast profile 224.1.1.1 simultaneously, then the counter of multicast profiles will be 3 but not 1.

❖ Configuring the Maximum Number of Global Profiles

Command	ip igmp snooping l2-entry-limit <i>number</i>
----------------	--

Parameter Description	<i>number</i> : Indicates the maximum number of multicast profiles.
Command Mode	Global configuration mode
Usage Guide	This value includes the number of both dynamic profiles as well as static profiles.

❖ Configuring Source Port Inspection

Command	ip igmp snooping source-check port
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After source port inspection is enabled, the multicast traffic received by a device will be discarded if no router port is detected in the network environment.

❖ Configuring Source IP Inspection

Command	ip igmp snooping source-check default-server <i>source-address</i>
Parameter Description	<i>source-address</i> : Indicates the source IP address.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Enabling Source IP Inspection for a Specific Profile

Command	ip igmp snooping limit-ipmc vlan <i>vid</i> address <i>group-address</i> server <i>source-address</i>
Parameter Description	<i>vid</i> vlan id <i>group-address</i> : Indicates a profile address. <i>source-address</i> : Indicates the source IP address.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Enabling Preview

Command	ip igmp snooping preview <i>profile-number</i>
Parameter Description	<i>profile number</i> : Indicates the range of multicast addresses allowed for preview. The value ranges from 1 to 1,024.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring the Preview Duration

Command	ip igmp snooping preview interval <i>num</i>
----------------	---

Parameter Description	<i>num</i> : Specifies the preview duration which ranges from 1s to 300s (60s by default).
Command Mode	Global configuration mode
Usage Guide	This configuration allows unauthorized users to receive multicast traffic within the preview duration. After the duration is met, the preview will be stopped; the preview can be resumed in 300s.

❖ Displaying the Per-Port Profile Filtering

Command	show ip igmp snooping interface									
Parameter Description	N/A									
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode									
Usage Guide	<p>If the function is configured, the profile will be displayed, for example:</p> <pre>Qtech#show ip igmp snooping interfaces gigabitEthernet 0/1</pre> <table border="1"> <thead> <tr> <th>Interface</th> <th>Filter profile number</th> <th>max-group</th> </tr> </thead> <tbody> <tr> <td>-----</td> <td>-----</td> <td>-----</td> </tr> <tr> <td>GigabitEthernet 0/1</td> <td>1</td> <td></td> </tr> </tbody> </table>	Interface	Filter profile number	max-group	-----	-----	-----	GigabitEthernet 0/1	1	
Interface	Filter profile number	max-group								
-----	-----	-----								
GigabitEthernet 0/1	1									

❖ Displaying the Per-VLAN Profile Filtering

Command	show ip igmp snooping vlan
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If the function is configured, the profile will be displayed, for example:</p> <pre>IGMP VLAN filter: 1</pre>

❖ Displaying the Maximum Number of Interface Profiles

Command	show ip igmp snooping interface						
Parameter Description	N/A						
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode						
Usage Guide	<p>If the maximum number of multicast addresses for a port is configured, the value will be displayed, for example:</p> <pre>Qtech#show ip igmp snooping interfaces gigabitEthernet 0/1</pre> <table border="1"> <thead> <tr> <th>Interface</th> <th>Filter profile number</th> <th>max-group</th> </tr> </thead> <tbody> <tr> <td>-----</td> <td>-----</td> <td>-----</td> </tr> </tbody> </table>	Interface	Filter profile number	max-group	-----	-----	-----
Interface	Filter profile number	max-group					
-----	-----	-----					

	GigabitEthernet 0/1	1	200
--	---------------------	---	-----

❖ Displaying the Maximum Number of Global Profiles

Command	show ip igmp snooping vlan
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If the function is configured, the profile will be displayed, for example: IGMP Snooping L2-entry-limit: 65536

❖ Displaying the Information of Source Port Inspection

Command	show ip igmp snooping vlan
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If source port inspection is enabled, the following information will be displayed: Source port check: Enable

❖ Displaying the Information of Source IP Inspection

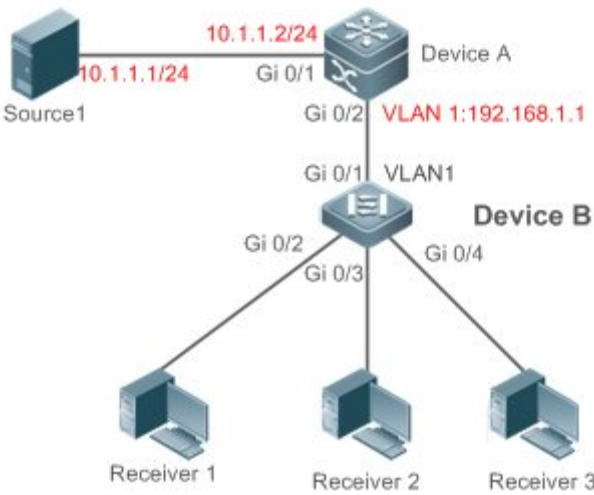
Command	show ip igmp snooping vlan
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If source IP address inspection is enabled, the following information will be displayed: Source ip check: Enable

❖ Displaying the Information of the Preview Function

Command	show ip igmp snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If the range of multicast addresses for a port is configured, preview will be enabled, for example: IGMP Preview: Enable IGMP Preview group aging time : 60(Seconds)

Configuration Example

❖ Configuring the Profile Filtering and the Maximum Number of Demanded Profiles

<p>Scenario Figure 9-9</p>	
	<p>A is the multicast router and is connected directly to multicast Source 1. B is a Layer-2 device and is connected directly to the user host and multicast Source 2. Receiver 1, Receiver 2, and Receiver 3 are connected to VLAN 1. By configuring VLAN 1, you can configure to allow the users within VLAN 1 to receive only the profiles whose addresses range from 225.1.1.1 to 225.1.255.255. You can configure Receiver 1 to receive only the profiles whose addresses range from 225.1.1.1 to 225.1.1.255, Receiver 2 to receive only the profiles whose addresses range from 225.1.2.1 to 255.1.2.255, and Receiver 3 to receive only the profiles whose addresses range from 225.1.3.1 to 225.1.3.255. At most 10 profiles can be added to a port and at most 100 profiles can be added globally.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure the IP address and VLAN. (Omitted) ➤ Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ➤ Enable IGMP snooping on B and select IVGL mode. ➤ Configure the range and maximum number of multicast addresses on B.
<p>A</p>	<pre>A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit</pre>

<p>B</p>	<pre>B# configure terminal B(config)#ip igmp snooping ivgl B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#rang B(config-profile)#range 225.1.1.1 225.1.255.255 B(config-profile)#exit B(config)#ip igmp profile 2 B(config-profile)#permit B(config-profile)#range 225.1.1.1 225.1.1.255 B(config-profile)#exit B(config)#ip igmp profile 3 B(config-profile)#permit B(config-profile)#range 225.1.2.1 225.1.2.255 B(config-profile)#exit B(config)#ip igmp profile 4 B(config-profile)#permit B(config-profile)#range B(config-profile)#range 225.1.3.1 225.1.3.255 B(config-profile)#exit B(config)#ip igmp snooping l2-entry-limit 100 B(config)#ip igmp snooping vlan 1 filter 1 B(config)#int gigabitEthernet 0/2 Qtech(config-if-GigabitEthernet 0/0)#ip igmp snooping filter 2 Qtech(config-if-GigabitEthernet 0/0)#ip igmp snooping max-groups 10 B(config)#int gigabitEthernet 0/3 Qtech(config-if-GigabitEthernet 0/0)#ip igmp snooping filter 3 Qtech(config-if-GigabitEthernet 0/0)#ip igmp snooping max-groups 10 B(config)#int gigabitEthernet 0/4 Qtech(config-if-GigabitEthernet 0/0)#ip igmp snooping filter 4 Qtech(config-if-GigabitEthernet 0/0)#ip igmp snooping max-groups 10</pre>
<p>Verification</p>	<p>➤ Run the show ip igmp snooping interfaces command to display the profile filtering and the maximum number of multicast profiles for a port.</p>

➤ Run the **show ip igmp snooping** command to display the maximum number of global multicast groups.

B

```
B#show ip igmp snooping interfaces
```

Interface	Filter profile number	max-group
GigabitEthernet 0/2	2	10
GigabitEthernet 0/3	3	10
GigabitEthernet 0/4	4	10

```
B#show ip igmp snooping
```

```
IGMP Snooping running mode: IVGL
```

```
IGMP Snooping L2-entry-limit: 100
```

```
Source port check: Disable
```

```
Source ip check: Disable
```

```
IGMP Fast-Leave: Disable
```

```
IGMP Report suppress: Disable
```

```
IGMP Globle Querier: Disable
```

```
IGMP Preview: Disable
```

```
IGMP Tunnel: Disable
```

```
IGMP Preview group aging time : 60(Seconds)
```

```
Dynamic Mroute Aging Time : 300(Seconds)
```

```
Dynamic Host Aging Time : 260(Seconds)
```

❖ Configuring Source Port Inspection

<p>Scenario Figure 9-10</p>	
	<p>A is the multicast router and is connected directly to multicast Source 1. B is a Layer-2 device and is connected directly to the user host and multicast Source 2. Receiver 1, Receiver 2, and Receiver 3 are connected to VLAN 1. Source 1 sends the multicast address traffic from profile 224.1.1.1, and Source 2 sends the multicast address traffic from profile 225.1.1.1. Receiver 1 can request profiles 224.1.1.1 and 225.1.1.1 respectively. Source port inspection is enabled.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Configure the IP address and VLAN. ➤ Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ➤ Enable IGMP snooping on B and select IVGL mode. ➤ Enable source port inspection on B.
<p>A</p>	<pre>A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit</pre>
<p>B</p>	<pre>B# configure terminal B(config)#ip igmp snooping ivgl B(config)#ip igmp snooping source-check port</pre>

<p>Verification</p>	<ul style="list-style-type: none"> ➤ Run the show ip igmp snooping mroute command to check whether Gi0/1 is learned as a router port. ➤ Check whether Receiver 1 can request the multicast traffic of profile 224.1.1 and cannot request that of profile 225.1.1.1.
<p>B</p>	<p>Multicast Switching Mroute Port</p> <p>D: DYNAMIC</p> <p>S: STATIC</p> <p>(* , * , 1):</p> <p>VLAN(1) 1 MROUTES:</p> <p>GigabitEthernet 0/1(S)</p> <p>B#show ip igmp snooping</p> <p>IGMP Snooping L2-entry-limit: 100</p> <p>Source port check: Enable</p> <p>Source ip check: Disable</p>

❖ Configuring Source IP Inspection

<p>Scenario Figure 9-11</p>	
	<p>A is the multicast router and is connected directly to multicast Source 1.</p> <p>B is a Layer-2 device and is connected directly to the user host and multicast Source 2.</p> <p>Receiver 1, Receiver 2, and Receiver 3 are connected to VLAN 1.</p> <p>Source 1 sends the multicast address traffic from profiles 10.1.1.1 and 224.1.1.1, Source 2 sends the multicast address traffic from profiles 192.168.1.3 and 225.1.1.1, and Source 3 sends the multicast address traffic from profiles 192.168.1.3 and 226.1.1.1.</p> <p>Receiver 1 can request profiles 224.1.1.1, 225.1.1.1, and 226.1.1.1 respectively.</p>

	<p>The default IP address for source IP inspection is 10.1.1.1. Configure limit-ipmc and the multicast traffic of profile 225.1.1.1, and set the legal source address as 192.168.1.3.</p>
Configuration Steps	<ul style="list-style-type: none"> ➤ Configure the IP address and VLAN. ➤ Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ➤ Enable IGMP snooping on B and select IVGL mode. ➤ Enable source port inspection on B.
A	<pre>A# configure terminal A(config)# ip multicast-routing A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit</pre>
B	<pre>B# configure terminal B(config)# ip igmp snooping ivgl B(config)# ip igmp snooping source-check default-server 10.1.1.1 B(config)# ip igmp snooping limit-ipmc vlan 1 address 225.1.1.1 server 192.168.1.3</pre>
Verification	<ul style="list-style-type: none"> ➤ Run the show ip igmp snooping command to check whether source IP inspection is enabled. ➤ Check whether Receiver 1 can request the multicast traffic of profile 224.1.1 and 225.1.1.1 and cannot request that of profile 226.1.1.1.
B	<pre>B#show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Enable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable</pre>

IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.
- The multicast router port is not learned, leading to failure to receive the multicast traffic.
- The IP address for source IP inspection is inconsistent with the multicast IP address, leading to failure to receive the multicast traffic.

9.4.6 Configuring an IGMP Profile

Configuration Effect

- Create an IGMP filtering profile.

Configuration Steps

- ❖ Creating a Profile
 - (Optional) Create an IGMP filtering profile.
- ❖ Configuring the Profile Range
 - (Optional) Configure the range of multicast profile addresses.
- ❖ Configuring the Profile Filtering
 - (Optional) Configure the filtering mode of profile to **permit** or **deny**.

Verification

- Run the **show running-config** command to check whether the preceding configurations take effect.

Related Commands

- ❖ Creating a Profile

Command	<code>ip igmp profile profile-number</code>
Parameter Description	<i>profile-number</i> : Indicates the number of a profile.
Command Mode	Global configuration mode
Usage Guide	

- ❖ Configuring the Profile Range

Command	<code>range low-ip-address [high-ip-address]</code>
----------------	---

Parameter	<i>low-ip-address</i> : Specifies the start address.
Description	<i>low-ip-address</i> : Specifies the end address. Only one address is configured by default.
Command Mode	Profile configuration mode
Usage Guide	You can configure multiple addresses. If the IP addresses of different ranges are consecutive, the addresses will be combined.

❖ Configuring the Profile Filtering

Command	deny
Parameter Description	N/A
Command Mode	Profile configuration mode
Usage Guide	If the filtering mode of profile is set to deny while the range of multicast profiles is not specified, no profile is to be denied, which means to permit all profiles.

❖ Configuring the Profile Filtering

Command	permit
Parameter Description	N/A
Command Mode	Profile configuration mode
Usage Guide	If the filtering mode of profile is set to permit while the range of multicast profiles is not specified, no profile is to be permitted, which means to deny all profiles.

Configuration Example

❖ Creating a Filtering Profile

Configuration Steps	➤ Create a filtering profile.
	<pre>B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#range B(config-profile)#range 224.1.1.1 235.1.1.1 B(config-profile)#</pre>
Verification	Run the show running-config command to check whether the configuration is successful.
	<pre>ip igmp profile 1 permit range 224.1.1.1 235.1.1.1</pre>

Configuration Steps	➤ Create a filtering profile.
	<pre>B(config)#ip igmp profile 1 B(config-profile)#permit B(config-profile)#range B(config-profile)#range 224.1.1.1 235.1.1.1 B(config-profile)#</pre>
Verification	Run the show running-config command to check whether the configuration is successful.
	!

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.
- The mode of profile is set to **permit** while the range of multicast profiles is not specified, leading to the denial of all profiles.

9.4.7 Configuring IGMP QinQ

Configuration Effect

- Create a multicast entry on the VLAN where IGMP packets are located. Forward IGMP packets on the VLAN where these packets are located, realizing transparent transmission.

Notes

- Basic IGMP snooping functions must be configured.

Configuration Steps

- ❖ Configuring QinQ Transparent Transmission
- If the QinQ interface needs to forward multicast packets on the VLANs where the VIDs of the packets specify, enable QinQ to realize transparent transmission.

Verification

- Run the **show ip igmp snooping** command to check whether the configuration takes effect.

Related Commands

- ❖ Configuring QinQ Transparent Transmission

Command	ip igmp snooping tunnel
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	Enable QinQ to realize transparent transmission of IGMP packets.
--------------------	--

❖ Displaying QinQ Configuration

Command	show ip igmp snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	If QinQ is enabled, the following content is displayed. <pre>IGMP Tunnel: Enable</pre>

Configuration Example

❖ Configuring QinQ Transparent Transmission

Configuration Steps	<ul style="list-style-type: none">➤ Configure basic IGMP snooping functions.➤ Configure QinQ transparent transmission. <pre>Qtech# configure terminal Qtech(config)# ip igmp snooping tunnel Qtech(config)# Qtech(config)# end</pre>
Verification	Run the show ip igmp snooping command to check whether the configuration is successful. <pre>IGMP Tunnel: Enable</pre>

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.

9.4.8 Configuring an IGMP Querier

Configuration Effect

- Configure the device as an IGMP querier, which will send IGMP Query packets periodically and collect user demanding information.

Notes

- Basic IGMP snooping functions must be configured.

Configuration Steps

- ❖ Enabling the Querier Function
 - (Optional) Enable IGMP querier function globally or for a specified VLAN.
 - (Optional) Disable the IGMP querier function for a specified VLAN.
- ❖ Configuring the Source IP Address of a Querier

- (Optional) You can configure the source IP address of a Query packet sent by the querier based on VLANs.
- After a querier is enabled, a source IP address must be specified for the querier; otherwise, the configuration will not take effect.
- ❖ Configuring the Maximum Response Time of a Query Packet
 - (Optional) Adjust the maximum response time carried by an IGMP Query packet. As IGMPv1 does not support the carrying of maximum response time by a Query packet, this configuration does not take effect when the querier is running IGMPv1.
- ❖ Configuring the Query Interval of a Querier
 - (Optional) Adjust the interval of the IGMP querier for sending query packets.
- ❖ Configuring the Aging Timer of a Querier
 - (Optional) Configure the aging timer of other IGMP queriers on the network.
- ❖ Specifying the IGMP Version for a Querier
 - (Optional) Specify the IGMP version for a querier (IGMPv2 by default).

Verification

- Run the **show ip igmp snooping querier detail** command to check whether the configuration takes effect.

Related Commands

- ❖ Enabling the IGMP Querier Function

Command	ip igmp snooping [vlan vid] querier
Parameter Description	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	IGMP querier for a specified VLAN will take effect only after global IGMP querier is enabled. If global IGMP querier is disabled, IGMP querier for all the VLANs will be disabled.

- ❖ Configuring the Source IP Address of a Querier

Command	ip igmp snooping [vlan vid] querier address a.b.c.d
Parameter Description	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default. a.b.c.d: Indicates the source IP address.
Command Mode	Global configuration mode
Usage Guide	After a querier is enabled, a source IP address must be specified for the querier; otherwise, the configuration will not take effect. If the source IP address is specified by a VLAN, the address will be used preferentially.

❖ Configuring the Maximum Response Time of a Querier

Command	ip igmp snooping [vlan vid] querier max-response-time seconds
Parameter Description	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default. seconds: Indicates the maximum response time. in the unit of seconds. The value ranges from 1 to 25.
Command Mode	Global configuration mode
Usage Guide	If the query interval is specified by a VLAN, the value will be used preferentially.

❖ Configuring the Query Interval of a Querier

Command	ip igmp snooping [vlan vid] querier address a.b.c.d
Parameter Description	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default. seconds: Indicates the query interval in the unit of seconds. The value ranges from 1 to 18,000.
Command Mode	Global configuration mode
Usage Guide	If the query interval is specified by a VLAN, the value will be used preferentially.

❖ Configuring the Aging Timer of a Querier

Command	ip igmp snooping [vlan vid] querier timer expiry seconds
Parameter Description	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default. seconds: Indicates the timeout time in the unit of seconds. The value ranges from 60 to 300.
Command Mode	Global configuration mode
Usage Guide	A device may fail to be elected as the querier even when its querier function is enabled. If a device that fails to be elected does not receive the Query packet sent by the querier in the aging time, the querier in use is considered as expired, and a new round of election will be raised. If the aging time is specified by a VLAN, the value will be used preferentially.

❖ Specifying the IGMP Version for a Querier

Command	ip igmp snooping [vlan vid] querier version 1
Parameter Description	vlan vid: Specifies a VLAN. This configuration applies to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	A querier can be run in IGMPv1 and IGMPv2 (IGMPv2 by default). You can also run a command to configure the version to IGMPv1. If the IGMP version for a querier is specified by a VLAN, the version will be used preferentially.

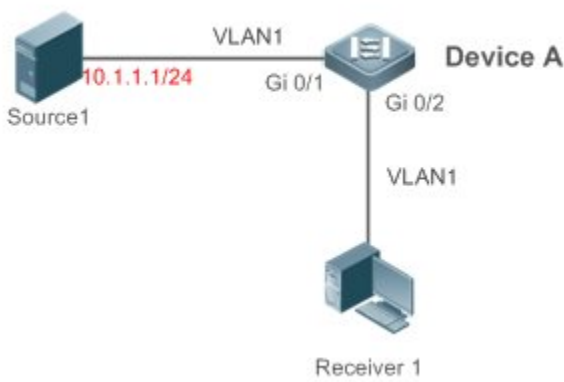
❖ Displaying the IGMP Querier Configuration

Command	show ip igmp snooping querier detail
Parameter Description	N/A

Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	<p>If QinQ is enabled, the following content is displayed.</p> <pre> Qtech(config)#show ip igmp snooping querier detail Vlan IP Address IGMP Version Port ----- Global IGMP switch querier status ----- admin state : Enable admin version : 2 source IP address : 1.1.1.1 query-interval (sec) : 60 max-response-time (sec) : 10 querier-timeout (sec) : 125 Vlan 1: IGMP switch querier status ----- admin state : Disable admin version : 2 source IP address : 1.1.1.1 query-interval (sec) : 60 max-response-time (sec) : 10 querier-timeout (sec) : 125 operational state : Disable operational version : 2 </pre>

Configuration Example

- ❖ Enabling the IGMP Querier Function

<p>Scenario Figure 9-12</p>	 <p>The diagram illustrates a network topology. On the left, a server icon labeled 'Source1' is connected to a central switch icon labeled 'Device A'. The connection is labeled 'VLAN1' and 'Gi 0/1'. The IP address '10.1.1.1/24' is shown next to Source1. On the right, 'Device A' is connected to a laptop icon labeled 'Receiver 1'. This connection is also labeled 'VLAN1' and 'Gi 0/2'.</p>
	<p>In the scenario without Layer-3 multicast equipment, the multicast traffic can be forwarded only on the Layer-2 network. A acts as a Layer-2 device to connect to the multicast source and receiver.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ➤ Enable global IGMP snooping on A in IVGL mode. ➤ Enable IGMP querier for VLAN 1 on A.
<p>A</p>	<pre>A(config)#ip igmp snooping ivgl A(config)#ip igmp snooping querier A(config)#ip igmp snooping querier address 10.1.1.1 A(config)#ip igmp snooping vlan 1 querier</pre>
<p>Verification</p>	<p>Run the show ip igmp snooping querier command to check whether the querier of VLAN 1 takes effect.</p>
<p>A</p>	<pre>A(config)#show ip igmp snooping querier Vlan IP Address IGMP Version Port ----- 1 10.1.1.1 2 switch A(config)#show ip igmp snooping querier vlan 1 Vlan 1: IGMP switch querier status ----- elected querier is 10.1.1.1 (this switch querier) ----- admin state : Enable</pre>

admin version	: 2
source IP address	: 10.1.1.1
query-interval (sec)	: 60
max-response-time (sec)	: 10
querier-timeout (sec)	: 125
operational state	: Querier
operational version	: 2

Common Errors

- The source IP address is not configured for the querier and the querier does not take effect.
-

9.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears the statistics on IGMP snooping.	clear ip igmp snooping statistics
Clears the dynamic router ports and member ports.	clear ip igmp snooping gda-table

Displaying

Description	Command
Displays basic IGMP snooping configurations.	show ip igmp snooping [vlan <i>vlan-id</i>]
Displays the statistics on IGMP snooping.	show ip igmp snooping statistics [vlan <i>vlan-id</i>]
Displays the router ports.	show ip igmp snooping mrouter
Displays the IGMP snooping entries.	show ip igmp snooping gda-table
Displays the profile.	show ip igmp profile [<i>profile-number</i>]
Displays the IGMP snooping configurations on an interface.	show ip igmp snooping interface <i>interface-name</i>
Displays the IGMP querier.	show ip igmp snooping querier [detail]
Displays user information.	show ip igmp snooping user-info

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs all IGMP Snooping functions.	debug igmp-snp
Debugs the IGMP snooping events.	debug igmp-snp event
Debugs the IGMP snooping packets.	debug igmp-snp packet
Debugs the communications between IGMP snooping and MSF.	debug igmp-snp msf
Debugs the IGMP snooping alarms.	debug igmp-snp warning

10. CONFIGURING MLD SNOOPING

10.1 Overview

Multicast Listener Discovery (MLD) Snooping is used to control and manage the forwarding behaviors of IPv6 multicast packets at Layer 2.

The device running MLD Snooping analyzes MLD packets received by a port to create a mapping between the port and the MAC multicast address and forwards IPv6 multicast data at Layer 2 based on the mapping. When MLD Snooping is disabled, IPv6 multicast data packets are broadcasted at Layer 2. When MLD Snooping is enabled, multicast data packets of a known IPv6 multicast group are forwarded to a specified receiver at Layer 2 instead of being broadcasted at Layer 2.

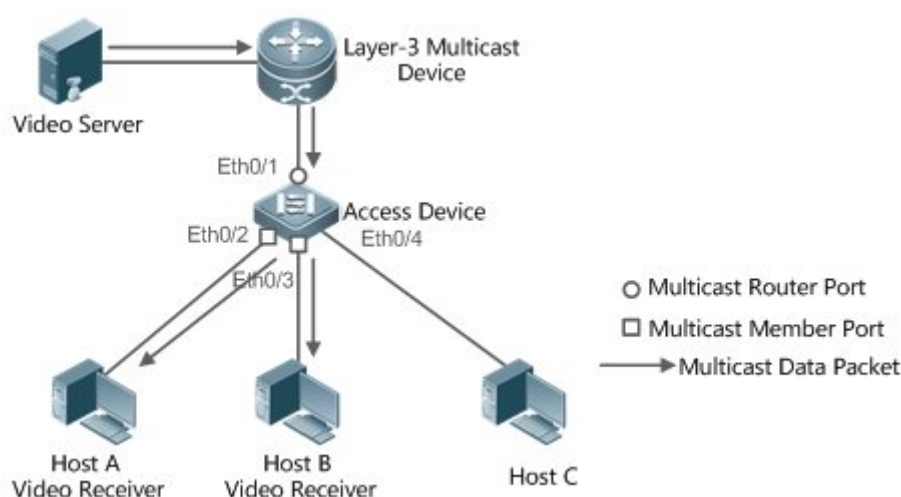
Protocols and Standards

RFC4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

10.1.1 Two Types of MLD Snooping Ports

As shown in Figure 10-1, the Layer-3 multicast device is connected to the multicast source. MLD Snooping is enabled on the access device. Host A and Host B are receivers (that is, members of the IPv6 multicast group).

Figure 10-1 Two Types of MLD Snooping Ports



- Multicast router port: Indicates the port on the access device for connecting to the Layer-3 multicast device, for example, Port Eth0/1 of the access device.
- Member port: Is short for IPv6 multicast group member port, also called listener port, and indicates the port on the access device for connecting to an IPv6 multicast group member, for example, Port Eth0/2 and Port Eth0/3 on the access device.

10.1.2 Work Mode of MLD Snooping

- **DISABLE mode:** MLD Snooping does not take effect in this mode. That is, the Layer-2 multicast device does not "snoop" MLD packets between the host and the router, and multicast streams are broadcasted within VLANs.
- **Independent VLAN Group Learn (IVGL) mode:** In this mode, multicast streams between VLANs are mutually independent. A host can request only the multicast router port in the same VLAN as the host to receive multicast packets, and can forward the received multicast data packets of any VLAN only to the member port and multicast router port in the same VLAN as the host.
- **Shared VLAN Group Learn (SVGL) mode:** In this mode, hosts of VLANs share the same multicast stream. A host in one VLAN can request multicast streams of another VLAN. When a shared VLAN is specified, only the multicast data streams of this VLAN can be forwarded to hosts of other VLANs. Multicast data streams of a shared VLAN, can be forwarded to the member ports of this multicast address, even though some member ports do not belong to the shared VLAN. In SVGL mode, MLD profiles must be used to allocate a batch of multicast address ranges to SVGL. Within the multicast address ranges, member ports in the multicast forwarding entries support trans-VLAN packet forwarding. By default, all the group ranges are not within the SVGL application ranges, and all the multicast packets are discarded.
- **IVGL-SVGL mode:** In this mode, IVGL and SVGL coexist. You can use MLD profiles to allocate a batch of multicast address ranges to SVGL. Within the multicast address ranges, member ports in the multicast forwarding entries support trans-VLAN packet forwarding. Member ports in the multicast forward entries corresponding to other multicast address ranges must belong to the same VLAN.

10.1.3 Working Principle of MLD Snooping

The device running MLD Snooping processes different MLD packets as follows:

MLD QUERY

The Layer-3 multicast device regularly sends an MLD General Query packet to all hosts and routers (with the address of FF02::1) in the local network segment, to query the IPv6 multicast group members in this network segment. When receiving the MLD General Query packet, the device running MLD Snooping forwards the packet all ports in the VLAN except the one receiving the packet, and processes the port receiving the packet as follows:

- If the port is already in the router multicast port list, its aging timer is reset.
- If the port is not contained in the router multicast port list, the port is added to the router multicast port list and its aging timer is started.
- Each time the Layer-2 multicast device receives an MLD General Query packet, it starts the aging timer for each member port, and updates the timer time to the configured maximum response time of MLD query packet. When the aging timer time of a port is reduced to 0, it is deemed that no member receives multicast streams through this port, and therefore, the Layer-2 multicast device deletes the port from the MLD Snooping forwarding table.

- Each time the Layer 2 multicast device receives a MLD Group-Specific Query packet, it starts the aging timer for each member port in the specific group, and updates the timer time to the configured maximum response time of MLD query packet. When the aging timer time of a port is reduced to 0, it is deemed that no member receives multicast streams through this port, and therefore, the Layer-2 multicast device deletes the port from the MLD Snooping forwarding table.
- When the Layer-2 multicast device receives a MLD Group-Specific Query packet, it no longer updates the preceding two types of timers.

MLD REPORT

In either of the following cases, the host sends an MLD Membership Report packet to the MLD querier.

- After receiving an MLD query (General Query or Group-Specific Query) packet, an IPv6 multicast group member host responds with an MLD Membership Report packet.
- If a host needs to join an IPv6 multicast group, it actively sends an MLD Membership Report packet to MLD querier to request to join this IPv6 multicast group.

When receiving an MLD Membership Report packet, the device running MLD Snooping forwards it to all multicast router ports in the VLAN, retrieves, from the packet, the address of the IPv6 multicast group that the host needs to join, and processes the port receiving the packet as follows:

- If there is no forwarding entry corresponding to the IPv6 multicast group, the forwarding entry is created, the port is added to the egress port list as a dynamic member port, and its aging timer is started.
- If there is a forwarding entry corresponding to the IPv6 multicast group but the port is not contained in the egress port list, the port is added to the egress port list as a dynamic member port, and its aging timer is started.
- If there is a forwarding entry corresponding to the IPv6 multicast group and dynamic member port is contained in the egress port list, its aging timer is reset.

MLD LEAVE

When a host leaves an IPv6 multicast group, it sends an MLD Leave packet (with the address of FF02::2) to notify the multicast router that it has left the IPv6 multicast group. When receiving an MLD Leave packet from a member port, the device running MLD Snooping directly forwards it to the multicast router port. If the fast leave function is enabled, the device directly deletes the port from the forwarding port list of the relevant multicast group.

10.1.4 Source Port Check

The source port check function of MLD Snooping improves the network security.

This function strictly limits the ingress ports of MLD multicast streams. When this function is disabled, multicast streams from any port are valid and the Layer-2 multicast device forwards them to registered member ports according to the forwarding list of MLD Snooping. When this function

is enabled, multicast streams only from the multicast router ports are valid and the Layer-2 multicast device forwards them to registered ports. Multicast data streams from non-multicast router ports are invalid and discarded.

10.2 Applications

Application	Description
MLD Snooping SVGL Trans-VLAN	MLD Snooping works in SVGL mode
Multicast On demand	
Source Port Filtering	Multicast streams only from multicast router ports are received.

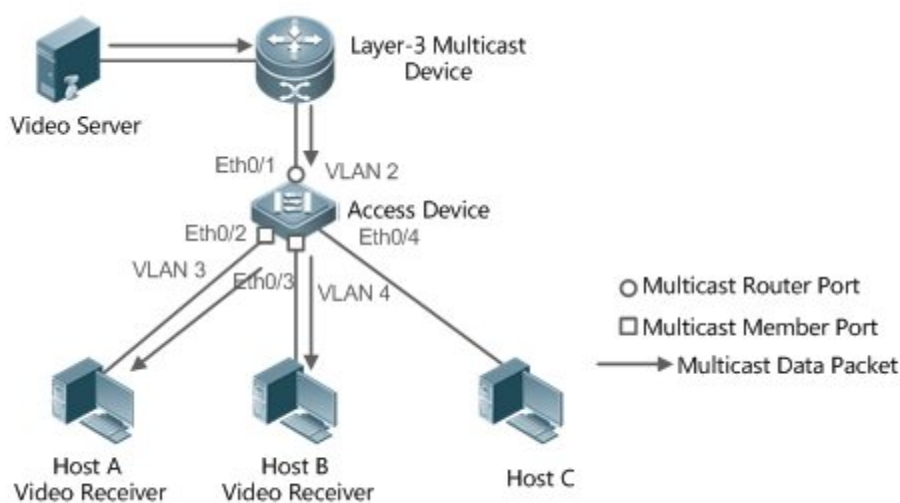
10.2.1 MLD Snooping SVGL Trans-VLAN Multicast On demand

Scenario

As shown in Figure 10-2, Host A of VLAN 3 and Host B of VLAN 4 order a video. The video streams are in VLAN 2.

- Enable the SVGL mode on the access device and set a shared VLAN 2.

Figure 10-2



Remark	VLAN 2 is a shared VLAN.
s	VLAN 3 and VLAN 4 are the VLANs through which the video on-demand service is output.

Deployment

- Enable the Layer-3 multicast protocol on the Layer-3 multicast device.
- Enable the SVGL mode on the Layer-2 device.

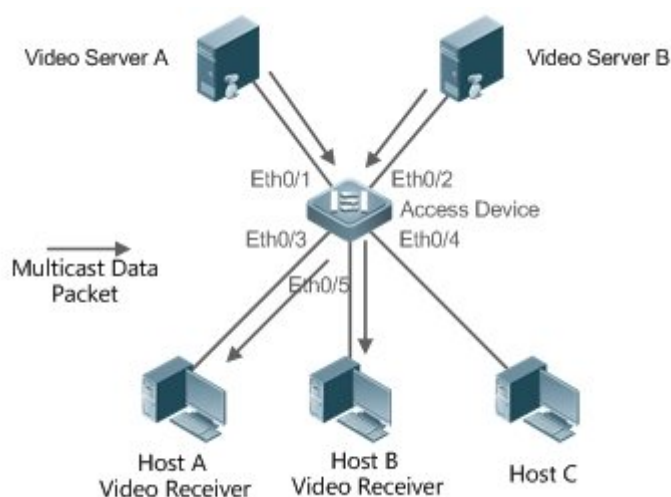
10.2.2 Source Port Filtering

Scenario

As shown in Figure 10-3, when the source port check function is configured, video streams can be received only from the source multicast router port. Multicast video streams from other ports are invalid and discarded. Note that when the source port check function is configured, there shall be at least one multicast router port. Otherwise, packet filtering is not performed on the multicast router port even though the source port filtering is enabled. When the source port check function is not configured, multicast video streams from all ports are received by default.

- Enable the IVGL mode on the access device.

Figure 10-3



Remark	Port Eth0/1 is a multicast router port and Port Eth0/2 is a non-multicast router port.
s	Video servers send same multicast video streams. Hosts A and B can receive multicast streams only from Video Server A.

Deployment

- Enable the source port check function and configure a static multicast router port.
- Enable the IVGL mode on the Layer-2 device.

10.3 Features

Basic Concepts

- ❖ Multicast Router Port and Member Port

Multicast router ports are classified into dynamic multicast router ports and static multicast router ports. If MLD Snooping is enabled, when the dynamic multicast router port learning function is

enabled on a port, after receiving an MLD Query or PIMv6-Hello packet, the port learns the dynamic multicast router port and starts the aging timer of the dynamic multicast router port. A static multicast router port can be added by configuring the **ipv6 mld snooping vlan mrouter** command.

Member ports are classified into dynamic member ports and static member ports. If MLD Snooping is enabled, after receiving an MLD Report packet, a port learns the dynamic member router port and starts the aging timer of the dynamic member port. A static member port can be added by configuring the **ipv6 mld snooping vlan static interface** command.

❖ Fast Leave and Packet Suppression

When the fast leave function is enabled, a port is directly deleted after receiving an MLD Leave packet. The fast leave function is applicable only to scenarios in which only one user is connected to a port, and helps save the bandwidth. When multiple users are connected to a port, if the fast leave function is enabled, other users wanting to receive packets fail to receive any packets.

When the packet suppression function is enabled, only the first MLD Report packet is forwarded within one query period.

Overview

Feature	Description
Globally Enabling MLD Snooping	Globally enables MLD Snooping and configures the work mode.
VLAN-based MLD Snooping	Enables or disables MLD Snooping for a single VLAN when MLD Snooping is globally enabled.
Aging Time of Multicast Router Ports	Adjusts the aging time of dynamic multicast router ports. The default aging time is 300s.
Dynamic Multicast Router Port Learning	After receiving an MLD query packet or a PIMv6 Hello packet, the port is learnt as a dynamic multicast router port.
Fast Leave of Multicast Group Member Ports	A member port can be quickly deleted, instead of being aged and deleted after the query interval of a Group-Specific Query expires.
MLD Report Packet Suppression	Only the first Report packet is processed within one query period, reducing the work load of the module.
Source Port Check	Multicast streams received only from a multicast router port can be forwarded. Packets received from non-multicast router ports cannot be forwarded.
Port-based Specific Multicast Group Filtering	Only multicast group packets that meet the filter conditions can be received.
Maximum Number of Multicast Groups Supported by a Port	Limits the maximum number of multicast groups that a port can join.

10.3.1 Globally Enabling MLD Snooping

Globally enable MLD Snooping and configure the work mode. Multicast forwarding entries can be learnt and multicast streams are forwarded to a specified port.

Working Principle

Enable MLD Snooping. When an MLD Report packet with the time to live (TTL) of 1 is received, a multicast forwarding entry is created and the forwarding egress is this port.

❖ Learning a Dynamic Member Port

After a valid MLD Report packet is received, a dynamic member port is learnt and a forwarding entry is generated. The forwarding egress of this entry is the member port.

❖ Coordinating Parameters

Configure the MLD Report packet suppression function.

Related Configuration

Configure the MLD Report packet suppression function so that only the first Report is processed within one query period, thereby reducing the number of packets in the network.

10.3.2 VLAN-based MLD Snooping

Enable or disable MLD Snooping for a single VLAN. By default, if MLD Snooping is globally enabled, the MLD Snooping function of each VLAN is enabled.

Related Configuration

Globally configure MLD Snooping. Then configure MLD Snooping for a single VLAN.

10.3.3 Aging Time of Multicast Router Ports

Multicast router ports are classified into dynamic multicast router ports and static multicast router ports. By default, the aging time of a dynamic multicast router port is 300s. Static multicast router ports are not aged.

Related Configuration

Ability of learning from dynamic multicast router port learning function

10.3.4 Dynamic Multicast Router Port Learning

By default, all ports support the dynamic multicast router port learning function.

Working Principle

When a port supports the dynamic multicast router port learning function, after receiving an MLD query packet or a PIMv6 Hello packet, the port is learnt as a dynamic multicast router port.

Related Configuration

Configure a port as a static multicast router port.

10.3.5 Aging Time of Dynamic Member Ports

Member ports are classified into dynamic member ports and static member ports. By default, the aging time of a dynamic member port is 260s. Static member ports are not aged.

10.3.6 Fast Leave of Multicast Group Member Ports

By default, the fast leave function of multicast group member ports are disabled. If the fast leave function is enabled, the port is directly deleted after receiving a done packet.

10.3.7 MLD Report Packet Suppression

By default, the MLD report packet suppression function is disabled. If the function is enabled, only the first Report packet is processed within one query interval, thereby reducing the number of packets in the network.

10.3.8 Source Port Check

The source port check function is disabled by default.

Working Principle

When the source port check function is enabled, packets only from multicast router ports are valid and packets from non-multicast router ports are invalid.

Related Configuration

Configure a port as a static multicast router port.

10.3.9 Port-based Specific Multicast Group Filtering

Under certain circumstances, you may use the port filtering function to control a port to forward multicast packets only of a certain range.

10.3.10 Maximum Number of Multicast Groups Supported by a Port

The maximum number of multicast groups that a port is allowed to join can control the maximum number of multicast groups supported by the port.

10.4 Configuration

Configuration	Description and Command
	<code>ipv6 mld snooping</code> Enables MLD Snooping and specifies the work mode.

Configuring Basic Functions of MLD Snooping	ipv6 mld snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i>	Configures the static multicast router port.
	ipv6 mld snooping vlan <i>vlan-id</i> static <i>ip-addr</i> interface <i>interface-id</i>	Configures a static member port.
	ipv6 mld profile <i>profile-num</i>	Configures a profile.
	ipv6 mld snooping source-check port	Configures source port check.
	ipv6 mld snooping filter <i>profile-num</i>	Configures multicast group filtering for a port.
	ipv6 mld snooping max-groups <i>num</i>	Configures the maximum number of multicast groups that a port can join.

10.4.1 Configuring Basic Functions of MLD Snooping

Configuration Effect

- Enable MLD Snooping and configure the work mode.

Notes

- Enable MLD Snooping and set the work mode to SVGL. The MLD Snooping SVGL mode cannot coexist with IPv4 or IPv6 Layer-3 multicasting.
- When the work mode is SVGL or IVGL-SVGL, a profile must be associated to specify the multicast group range in which the SVGL mode applies.

Configuration Steps

- ❖ Enabling IPv6 MLD Snooping
 - Mandatory.

Verification

Run the **show ipv6 mld snooping** command to check whether MLD Snooping is enabled.

- Check whether the device can create correct multicast forwarding entries.

Related Commands

- ❖ Enabling IPv6 MLD Snooping

Command	ipv6 mld snooping <i>mode</i>
Parameter Description	mode: Specifies the work mode.
Command Mode	Global configuration mode
Usage Guide	N/A

- ❖ Configuring a Profile

Command	ipv6 mld profile <i>profile-num</i>
----------------	--

Parameter Description	<i>profile-num</i> : Indicates the profile number.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a profile and enter the profile configuration mode.

❖ Configuring a Static Multicast Router Port

Command	ipv6 mld snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i>
Parameter Description	vlan-id : Indicates the VLAN ID. <i>interface-id</i> : Indicates interface changes.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring a Static Member Port

Command	ipv6 mld snooping vlan <i>vlan-id</i> static <i>ip-addr</i> interface <i>interface-id</i>
Parameter Description	vlan-id : Indicates the VLAN ID. <i>ip-addr</i> : Indicates the group address. <i>interface-id</i> : Indicates interface changes.
Command Mode	Global configuration mode
Usage Guide	N/A

❖ Configuring Source Port Check

Command	ipv6 mld snooping source-check port
Parameter Description	
Command Mode	Global configuration mode
Usage Guide	-

❖ Configuring Port-based Multicast Group Filtering

Command	ipv6 mld snooping filter <i>profile-num</i>
Parameter Description	<i>profile-num</i> : Indicates the profile number.
Command Mode	Interface configuration port
Usage Guide	N/A

❖ Configuring the Maximum Number of Multicast Groups Supported by a Port

Command	ipv6 mld snooping max-groups <i>num</i>
Parameter Description	<i>num</i> : Indicates the number of groups.

Command Mode	Interface configuration port
Usage Guide	N/A

❖ Configuring Report Packet Suppression

Command	ipv6 mld snooping suppression enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	<p>When the Report packet suppression function is enabled, only the first Report packet of a specific VLAN and group is forwarded to a multicast router port within one query interval. The subsequent Report packets are forwarded to the multicast router port, so as to reduce the number of packets in the network.</p> <p>This function can only suppress the Report packets of MLDv1. It is invalid on the Report packets of MLDv2.</p>

❖ Configuring Port Fast Leave

Command	ipv6 mld snooping fast-leave enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	<p>When the port fast leave function is enabled, after receiving a Leave packet, the port is directly deleted from the member ports in the corresponding forwarding entries. Later, when receiving a relevant Group-Specific Query packet, the device does not forward the packet to this port. The Leaver packet includes the Leave packet of MLDv1, include type of MLDv2, and Report packet containing no source address.</p> <p>This function is applicable only to scenarios in which only one user is connected to a port, and helps save bandwidth and resources.</p>

❖ Configuring Dynamic Multicast Router Port Learning

Command	ipv6 mld snooping [vlan vid] mrouter learn
Parameter Description	vlan-id: Specifies a VLAN ID. This function is applicable to all VLANs by default.
Command Mode	Global configuration mode
Usage Guide	A multicast router port is a port that directly connects an MLD Snooping-enabled multicast device to a neighbor multicast device in which a multicast routing protocol is enabled. By default, when the dynamic multicast router port learning function is enabled, the device automatically listens to the MLD Query/PIM Hello packet and dynamically identifies a multicast router port.

❖ Configuring Aging Time of Dynamic Multicast Router Ports

Command	ipv6 mld snooping dyn-mr-aging-time <i>seconds</i>
Parameter Description	seconds: Indicates the aging time of dynamic multicast router ports. The unit is second and the value ranges from 1 to 3,600.
Command Mode	Global configuration mode
Usage Guide	<p>If a dynamic multicast router port does not receive an MLD General Query packet or a PIM Hello packet before the timeout of its aging time, the device deletes the port from the multicast router port list.</p> <p>When the dynamic multicast router learning function is enabled, you can use this command to adjust the aging time of dynamic multicast router ports. If the aging time is too short, a multicast router port may be added and deleted frequently.</p>

❖ Configuring Aging Time of Dynamic Member Ports

Command	ipv6 mld snooping host-aging-time <i>seconds</i>
Parameter Description	seconds: Indicates the aging time.
Command Mode	Global configuration mode
Usage Guide	<p>The aging time of a dynamic member port refers to the aging time set when a dynamic member port of a device receives from the host an MLD packet of joining a certain IPv6 multicast group.</p> <p>After receiving an MLD Join packet from a dynamic member port, the device resets the aging timer of the dynamic member port and sets the timer time to host-aging-time. If the timer times out, it is deemed that no user host receives multicast packets through this port, and then the multicast device deletes the port from the MLD Snooping member port list. After this command is configured, the aging timer value of dynamic member ports when MLD Join packets are received subsequently is host-aging-time. The aging time takes effect immediately after configuration and the timers of started member ports are updated.</p>

❖ Configuring Response Time of Query Packets

Command	ipv6 mld snooping query-max-response-time <i>seconds</i>
Parameter Description	seconds: Indicates the response time.
Command Mode	Global configuration mode
Usage Guide	<p>After receiving an MLD General Query packet from a port, the multicast device resets the aging timers of all dynamic member ports and sets the timer time to query-max-response-time. If the timer times out, it is deemed that no user host receives multicast packets through the port, and then the multicast device deletes the port from the MLD Snooping member port list.</p> <p>After receiving an MLD Group-Specific Query packet from a port, the multicast device resets the aging timers of all dynamic member ports in the specific group and sets the timer time to query-max-response-time. If the timer times out, it is deemed that no user host receives multicast packets through the port, and then the multicast device deletes the port from the MLD Snooping member port list.</p>

The configuration takes effect when the a query packet is received next time, and the configuration of currently started timers are not updated. For Group-Specific Query packets of MLDv2, timers are not updated.

❖ Checking Multicast Router Ports

Command	show ipv6 mld snooping mroute
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode
Usage Guide	<p>If a multicast router port is successfully configured, the mark "S" is shown in the interface information displayed. For example:</p> <pre>Qtech(config)#show ipv6 mld snooping mrouter Multicast Switching Mroute Port D: DYNAMIC S: STATIC (*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/1(S)</pre>

❖ Checking Dynamic Multicast Router Port Learning

Command	show ipv6 mld snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode
Usage Guide	<p>Run the show ip igmp snooping command to check the aging time and learning status of dynamic multicast router ports.</p> <pre>Dynamic Mroute Aging Time : 300(Seconds) Multicast router learning mode: Enable</pre>

❖ Checking Member Ports

Command	show ipv6 mld snooping gda-table
Parameter Description	-
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode
Usage Guide	<p>If a member port is successfully configured, the mark "S" is shown in the interface information displayed. For example:</p>

```
Qtech(config)#show ipv6 mld snooping gda table
Multicast Switching Cache Table
D: DYNAMIC
S: STATIC
M: MROUTE
(*, FF15::100, 1):
VLAN(1) 2 OPORTS:
GigabitEthernet 3/7(S)
```

❖ Checking Other Parameters

Command	show ipv6 mld snooping
Parameter Description	-
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode
Usage Guide	<p>Run the show ipv6 mld snooping command to check the aging time of multicast router ports, aging time of dynamic member ports, response time of query packet, and Report packet suppression, and fast leave parameters.</p> <pre>MLD snooping mode: IVGL Source port check: Disable MLD Fast Leave: Disable MLD Report suppress: Disable Query Max Response Time: 10 (Seconds) Dynamic Mroute Aging Time: 300(Seconds) Dynamic Host Aging Time: 260(Seconds)</pre>

10.5 Monitoring

Clearing

Running the **clear** commands may lose vital information and thus interrupt services.

Description	Command
Clears MLD Snooping multicast forwarding entries.	clear ipv6 mld snooping gda-table
Clears MLD Snooping statistics.	clear ipv6 mld snooping statistics

Displaying

Description	Command
Displays the current MLD Snooping mode.	show ipv6 mld snooping
Displays MLD Snooping forwarding entries.	show ipv6 mld snooping gda-table
Displays MLD Snooping statistics.	show ipv6 mld snooping statistics
Displays MLD Snooping multicast router ports.	show ipv6 mld snooping mrouter
Displays MLD Snooping interface information, interface filtering profiles and maximum number of groups that a port can join.	show ipv6 mld snooping interfaces <i>interface-type interface-name</i>
Displays multicast information about a single VLAN, on which MLD Snooping is configured.	show ipv6 mld snooping vlan <i>vid</i>
Displays an MLD Profile.	show ipv6 mld profile <i>profile-number</i>