

Table of Contents

Chapter 1 IP Multicast Overview	1-1
1.1 IP Multicast Overview	1-1
1.2 Multicast Addresses.....	1-2
1.2.1 IP Multicast Addresses.....	1-2
1.2.2 Ethernet Multicast MAC Addresses	1-4
1.3 IP Multicast Protocols	1-4
1.3.1 Internet Group Management Protocol.....	1-5
1.3.2 Multicast Routing Protocol	1-5
1.4 IP Multicast Packet Forwarding	1-6
1.5 Application of Multicast.....	1-7
Chapter 2 IGMP Snooping Configuration	2-1
2.1 IGMP Snooping Overview	2-1
2.1.1 IGMP Snooping Principle	2-1
2.1.2 Implement IGMP Snooping	2-2
2.2 IGMP Snooping Configuration	2-4
2.2.1 Enabling/Disabling IGMP Snooping	2-4
2.2.2 Configuring Router Port Aging Time	2-5
2.2.3 Configuring Maximum Response Time	2-5
2.2.4 Configuring Aging Time of Multicast Group Member	2-6
2.3 Displaying and debugging IGMP Snooping.....	2-6
2.4 IGMP Snooping Configuration Example.....	2-7
2.4.1 Enable IGMP Snooping.....	2-7
2.5 IGMP Snooping Fault Diagnosis and Troubleshooting.....	2-7
Chapter 3 Common Multicast Configuration.....	3-1
3.1 Introduction to Common Multicast Configuration.....	3-1
3.2 Common Multicast Configuration.....	3-1
3.2.1 Enabling Multicast	3-1
3.2.2 Configuring Number Limit of Multicast Routing Entries	3-1
3.2.3 Clearing MFC Forwarding Entries or Its Statistic Information.....	3-2
3.2.4 Clearing Route Entries From the Core Multicast Routing Table	3-2
3.3 Displaying and debugging Common Multicast Configuration	3-3
Chapter 4 IGMP Configuration	4-1
4.1 IGMP Overview.....	4-1
4.2 Introduction to IGMP Proxy.....	4-2
4.3 IGMP Configuration	4-3
4.3.1 Enabling Multicast	4-4

4.3.2 Enabling IGMP on an Interface	4-4
4.3.3 Configuring IGMP Proxy	4-4
4.3.4 Configuring the IGMP Version	4-5
4.3.5 Configuring the Interval for Querying IGMP Packets	4-5
4.3.6 Configuring the Interval and the Number of Querying IGMP Packets	4-6
4.3.7 Configuring the limit of IGMP groups on an interface	4-7
4.3.8 Configuring a Router to Join Specified Multicast Group	4-7
4.3.9 Limiting Multicast Groups An Interface Can Access	4-8
4.3.10 Configuring the Interval to Send IGMP Query Message.....	4-9
4.3.11 Configuring the Present Time of IGMP Querier	4-9
4.3.12 Configuring Maximum Response Time for IGMP Query Message.....	4-9
4.3.13 Deleting IGMP Groups Joined on an Interface	4-10
4.4 Displaying and debugging IGMP	4-10
Chapter 5 PIM-DM Configuration	5-1
5.1 PIM-DM Overview.....	5-1
5.2 PIM-DM Configuration	5-2
5.2.1 Enabling Multicast	5-3
5.2.2 Enabling PIM-DM	5-3
5.2.3 Entering the PIM View.....	5-3
5.2.4 Configuring Sending Interval for the Hello Packets	5-4
5.2.5 Configuring the Filtering of Multicast Source/Group	5-4
5.2.6 Configuring the Filtering of PIM Neighbor.....	5-5
5.2.7 Configuring the Maximum Number of PIM Neighbor on an Interface.....	5-5
5.2.8 Clearing multicast route entries from PIM routing table	5-5
5.2.9 Clearing PIM Neighbors	5-6
5.3 Displaying and debugging PIM-DM	5-6
5.4 PIM-DM Configuration Example	5-7
Chapter 6 PIM-SM Configuration	6-1
6.1 PIM-SM Overview	6-1
6.1.1 Introduction to PIM-SM	6-1
6.1.2 PIM-SM Operating Principle.....	6-1
6.1.3 Preparations before Configuring PIM-SM	6-2
6.2 PIM-SM Configuration	6-3
6.2.1 Enabling Multicast	6-3
6.2.2 Enabling PIM-SM	6-3
6.2.3 Configuring the PIM-SM Domain Border	6-4
6.2.4 Entering the PIM view	6-4
6.2.5 Configuring Candidate-BSRs	6-5
6.2.6 Configuring Candidate-RPs	6-6
6.2.7 Configuring Static RP.....	6-6
6.2.8 Configuring the sending interval for the Hello packets of the interface.....	6-6
6.2.9 Configuring the filtering of multicast source/group.....	6-7

6.2.10 Configuring the filtering of PIM neighbor.....	6-7
6.2.11 Configuring the maximum number of PIM neighbor on an interface	6-7
6.2.12 Configuring RP to Filter the Register Messages Sent by DR	6-7
6.2.13 Limiting the range of legal BSR.....	6-8
6.2.14 Limiting the range of legal C-RP	6-9
6.2.15 Clearing multicast route entries from PIM routing table	6-9
6.2.16 Clearing PIM Neighbors	6-9
6.3 Displaying and debugging PIM-SM	6-9
6.4 PIM-SM Configuration Example	6-10

Chapter 1 IP Multicast Overview

Note:

When running IP multicast protocols, Ethernet switches also provide the functions of switches. We use routers in this manual to stand for not only the common routers but also the layer 3 Ethernet switches running IP multicast protocols.

1.1 IP Multicast Overview

Various transmission methods can be used when the destination of the information (including data, voice and video) is the minority part of users on the network. The unicast mode can be used, i.e., you should establish an independent data transmission path for each user. Or the broadcast mode can be used, i.e., you should send the information to all users on the network. No matter whether the users need the information, they will receive it from the broadcast. For example, if the same information is required by 200 users on the network, the traditional solution is to send the information 200 times respectively in unicast mode so that these users can receive the data they need. In the broadcast mode, the data is broadcast over the entire network. Users who need the data can get it directly on the network. Both of the methods greatly waste the precious bandwidth resources. In addition, the broadcast mode cannot ensure security and secrecy of the information.

Emergence of the IP multicast technology solves the problem in time. The multicast source sends the information only once. Multicast routing protocols establish tree-type routing for multicast packets. The information being sent will be replicated and distributed at the cross as far as possible (see Figure1-1). Therefore, the information can be correctly sent to each user who needs it with high efficiency.

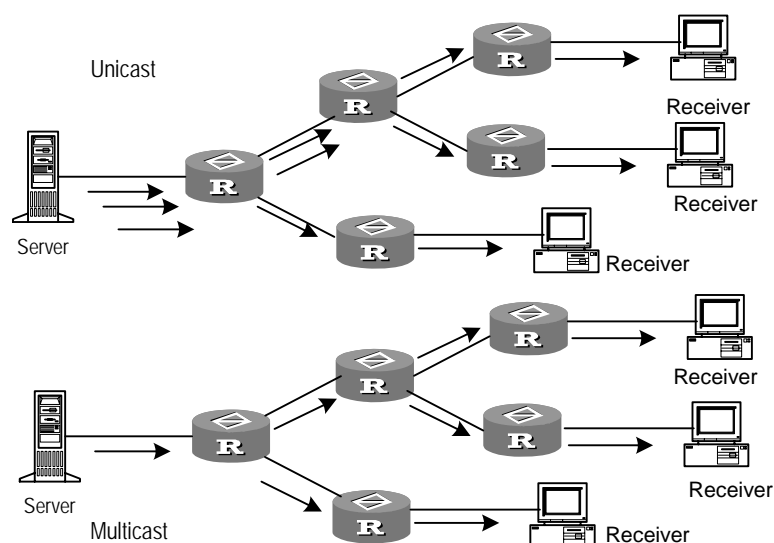


Figure 1-1 Comparison between the unicast and multicast transmission

It should be noted that a multicast source does not necessarily belong to a multicast group. It only sends data to the multicast group and it is not necessarily a receiver. Multiple sources can send packets to a multicast group simultaneously.

A router that does not support multicast may exist on the network. A multicast router can encapsulate the multicast packets in unicast IP packets with tunneling and send them to the neighboring multicast router. The neighboring multicast router will remove the unicast IP header and continue the multicast transmission. This avoids the network architecture from changing greatly.

Multicast advantages:

- Enhanced efficiency: Reduce network traffic and relieve server and CPU loads.
- Optimized performance: Decrease traffic redundancy.
- Distributed applications: Make multipoint applications possible.

1.2 Multicast Addresses

1.2.1 IP Multicast Addresses

The destination addresses of multicast packets use Class D IP addresses ranging from 224.0.0.0 to 239.255.255.255. Class D addresses cannot appear in the source IP address fields of IP packets.

During unicast data transmission, a packet is transmitted along a path from the source address to the destination address with the "hop-by-hop" principle on the IP network. However, in environments of IP multicast, a packet has more than one destination

address, i.e., a group of addresses. All the information receivers join a group. Once a receiver joins the group, data flowing to the group is sent to the receiver immediately. All members in the group can receive the packets. Membership of a multicast group is dynamic, that is, hosts can join and leave groups at any time.

A multicast group can be either permanent or temporary. Part of addresses in the multicast group is allocated by the official, known as the permanent multicast group. IP addresses of a permanent group keep unchanged but the members in the group can change. The number of members in a permanent multicast group can be random or even 0. Those IP multicast addresses that are not reserved for permanent multicast groups can be used by temporary groups.

Ranges and meanings of Class D addresses are shown in Table 1-1.

Table 1-1 Ranges and meanings of Class D addresses

Class D address range	Meaning
224.0.0.0~224.0.0.255	Reserved multicast addresses (addresses of permanent groups). Address 224.0.0.0 is reserved. The other addresses can be used by routing protocols.
224.0.1.0~238.255.255.255	Multicast addresses available for users (addresses of temporary groups). They are valid in the entire network.
239.0.0.0~239.255.255.255	Multicast addresses for local management. They are valid only in the specified local range.

Reserved multicast addresses that are commonly used are shown in the following table:

Table 1-2 Reserved multicast address list

Class D address	Meaning
224.0.0.0	Base Address (Reserved)
224.0.0.1	Addresses of all hosts
224.0.0.2	Addresses of all multicast routers
224.0.0.3	Unassigned
224.0.0.4	DVMRP routers
224.0.0.5	OSPF routers
224.0.0.6	OSPF DR (designated router)
224.0.0.7	ST routers
224.0.0.8	ST hosts

Class D address	Meaning
224.0.0.9	RIP-2 routers
224.0.0.10	IGRP routers
224.0.0.11	Mobile agents
224.0.0.12	DHCP server/Relay agent
224.0.0.13	All PIM routers
224.0.0.14	RSVP encapsulation
224.0.0.15	All CBT routers
224.0.0.16	Designated SBM
224.0.0.17	All SBMS
224.0.0.18	VRRP
.....

1.2.2 Ethernet Multicast MAC Addresses

When unicast IP packets are transmitted on the Ethernet, the destination MAC address is the MAC address of the receiver. However, when multicast packets are transmitted, the destination is no longer a specific receiver but a group with unspecific members. Therefore, the multicast MAC address should be used. Multicast MAC addresses are correspondent to multicast IP addresses. IANA (Internet Assigned Number Authority) stipulates that higher 24 bits of the multicast MAC address are 0x01005e and the lower 23 bits of the MAC address is the lower 23 bits of the multicast IP address.

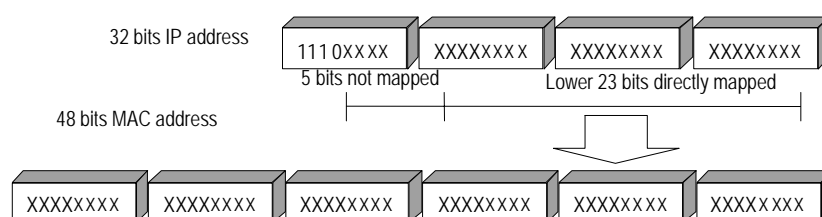


Figure 1-2 Mapping between the multicast IP address and the Ethernet MAC address

Because only 23 bits of the last 28 bits in the IP multicast address are mapped into the MAC address, 32 IP multicast addresses are mapped into the same MAC address.

1.3 IP Multicast Protocols

Multicast involves the multicast group management protocol and multicast routing protocol. At present, the multicast group management protocol uses the IGMP that is used as IP multicast basic signaling protocol. It is run between hosts and routers, enabling routers to know whether there are members of the multicast group on the network segment. The multicast routing protocol is running between multicast routers, creating and maintaining multicast routes and implementing correct and high-efficient multicast packet forwarding. At present, multicast routing protocols supported by S3900 Series include PIM-SM, PIM-DM.

1.3.1 Internet Group Management Protocol

Internet Group Management Protocol is the only protocol that hosts can use. It defines the membership establishment and maintenance mechanism between hosts and routers and is the basis of the entire IP multicast. Hosts report the group membership to a router through IGMP and inform the router of the conditions of other members in the group through the directly connected host. If a user on the network joins a multicast group through IGMP declaration, the multicast router on the network will transfer the information of membership to the multicast routing protocol. Finally, the network will be added to the multicast tree as a branch. When the host, as a member of a multicast group, begins receiving the information, the router will query the group periodically to check whether members in the group are involved. As long as one host is involved, the router will continue to send data. When all users on the network quit the multicast group, the related branches are removed from the multicast tree.

1.3.2 Multicast Routing Protocol

A multicast group address is a virtual address. Unicast allows packets to be routed from the data source to the specified destination address, which is impossible for multicast. The multicast application sends the packets to a group of receivers (with multicast addresses) who want to receive the data but not only to one receiver (with unicast address).

The multicast routing protocol creates a loop-free data transmission path from one data source to multiple receivers. The task of the multicast routing protocol is to build up the distribution tree architecture. A multicast router can use multiple methods to build up a path for data transmission, i.e., the distribution tree.

- PIM-DM (Protocol-Independent Multicast Dense Mode, PIM-DM)

PIM dense mode is suitable for small networks. It assumes that each subnet in the network contains at least one receiver who is interested in the multicast source. Therefore, multicast packets are flooded to all points of the network. Subsequent

resources related (such as bandwidth and CPU of routers) will be consumed. In order to decrease the consumption of these precious network resources, branches that do not have members send Prune messages toward the source to prune off the unwanted/unnecessary traffic. To enable the receivers in the pruned branches who have multicast data forwarding requirement to receive multicast data streams, the pruned branches can be restored to forwarding state periodically. To reduce the latency time during which the pruned branches wait for being restored, PIM dense mode uses the graft mechanism to actively restore the forwarding of multicast packets. The periodical flood and prune are characteristics of PIM dense mode. Generally, the forwarding path in dense mode is a “source tree” rooted at the source with multicast members as the branches. Since the source tree uses the shortest path from the multicast source and the receiver, it is also called the shortest path tree (SPT).

- PIM-SM (Protocol-Independent Multicast Sparse Mode, PIM-SM)

Dense mode uses the flood-prune technology, which is not applicable for WAN. In WAN, multicast receivers are sparse and the sparse mode are mostly used. In sparse mode, all hosts do not need to receive multicast packets unless there is an explicit request for the packets by default. A multicast router must send a join message to the RP (Rendezvous Point, which needs to be built up in the network and is the virtual place for data exchange) corresponding to the group to receive the multicast data traffic from the specified group. The join message passes routers hop by hop and finally reaches the root, i.e., the RP. The path the join message passed becomes a branch of the shared tree. In PIM sparse mode, multicast packets are sent to the RP first and then are forwarded along the shared tree rooted at the RP and with members as the branches. To prevent the branches of the shared tree from being deleted for they not updated, the PIM-SM protocol sends join messages to branches periodically to maintain the multicast distribution tree.

To send data to the specified address, senders should register with the RP first before forwarding data to the RP. When the data reaches the RP, the multicast packets are replicated and sent to receivers along the path of the distribution tree. Replicate only happens at the branches of the distribution tree. This process can be automatically repeated until the packets reach the destination.

1.4 IP Multicast Packet Forwarding

In the multicast model, the source host sends information to the host group represented by the multicast group address within the destination address fields of the IP packets. Different from the unicast model, the multicast model must forward the multicast packets to multiple external interfaces so that the packets can be sent to all receivers. Therefore, the multicast forwarding process is much more complex than the unicast forwarding process.

- RPF (Reverse Path Forwarding)

To ensure that a multicast packet reaches the router along the shortest path, the multicast must depend on the unicast routing table or a multicast routing table independently provided for multicast to check the receiving interface of multicast packets. This check mechanism is the basis for most multicast routing protocols performing multicast forwarding, which is known as RPF (Reverse Path Forwarding) check. A multicast router uses the source address at which the multicast packet arrives to query the unicast routing table or the independent multicast routing table so as to determine that the incoming interface at which the packet arrives is on the shortest path from the receiver to the source address. If a source tree is used, the source address is the address of the source host sending the multicast packet. If a shared tree is used, the source address is the address of the root of the shared tree. When a multicast packet arrives at the router, if RPF check succeeds, the packet will be forwarded according to the multicast forwarding entry. Otherwise, the packet will be dropped.

1.5 Application of Multicast

IP multicast technology effectively solves the problem of packet forwarding from single-point to multi-point. It implements high-efficient data transmission from single-point to multi-point in IP networks and can save a large amount of network bandwidth and reduce network loads. New value-added services that take advantage of multicast can be delivered in the Internet information service area including direct broadcasting, Web TV, distance learning, distance medicine, net broadcasting station and real-time audio/video conferencing.

- Multimedia and streaming media applications
- Communications of the training and corporate sites
- Data repository and finance (stock) applications
- Any "point-to-multipoint" data distribution

With the increase of multimedia services on IP networks, multicast has huge market potential and multicast services will become popular gradually.

Chapter 2 IGMP Snooping Configuration

2.1 IGMP Snooping Overview

2.1.1 IGMP Snooping Principle

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast control mechanism running on the Layer 2 Ethernet switch and it is used for multicast group management and control.

IGMP Snooping runs on the link layer. When receiving the IGMP messages transmitted between the host and router, the Layer 2 Ethernet switch uses IGMP Snooping to analyze the information carried in the IGMP messages. If the switch hears IGMP host report message from an IGMP host, it will add the host to the corresponding multicast table. If the switch hears IGMP leave message from an IGMP host, it will remove the host from the corresponding multicast table. The switch continuously listens to the IGMP messages to create and maintain MAC multicast address table on Layer 2. And then it can forward the multicast packets transmitted from the upstream router according to the MAC multicast address table.

When IGMP Snooping is disabled, the packets are broadcast on Layer 2. See the following figure:

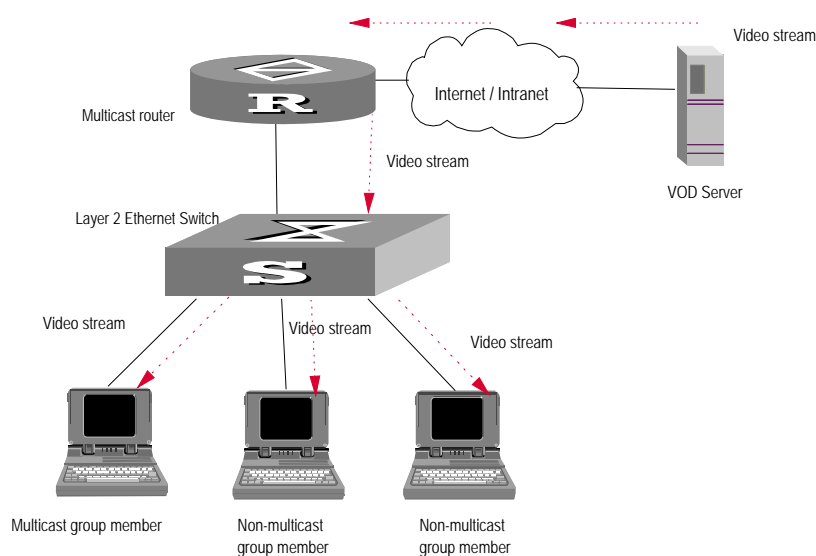


Figure 2-1 Multicast packet transmission without IGMP Snooping

When IGMP Snooping runs, the packets are not broadcast on Layer 2. See the following figure:

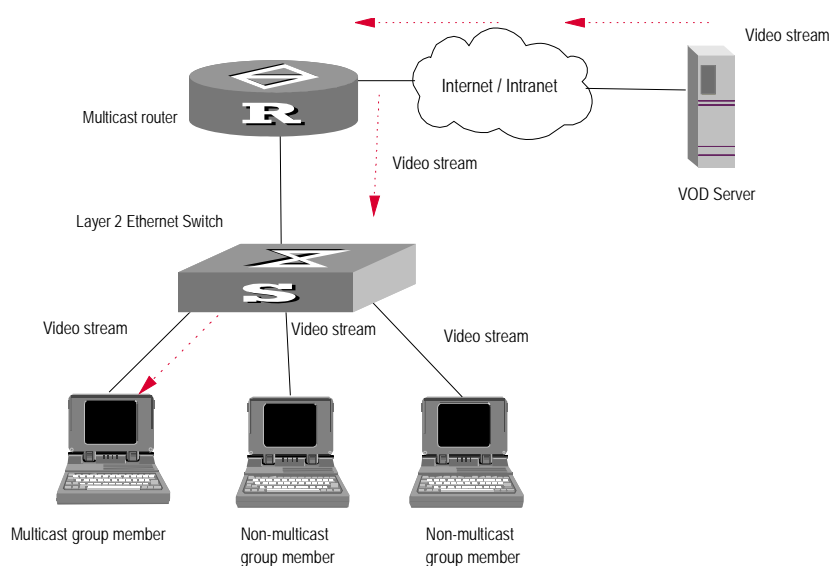


Figure 2-2 Multicast packet transmission when IGMP Snooping runs

2.1.2 Implement IGMP Snooping

I. Related concepts of IGMP Snooping

To facilitate the description, this section first introduces some related switch concepts of IGMP Snooping:

- Router Port: The port of the switch, directly connected to the multicast router.
- Multicast member port: The port connected to the multicast member. The multicast member refers to a host joined a multicast group.
- MAC multicast group: The multicast group is identified with MAC multicast address and maintained by the Ethernet switch.
- Router port aging time: Time set on the router port aging timer. If the switch has not received any IGMP general query, PIM hello or DVMRP probe message before the timer times out, it considers the port no longer as a router port.
- Multicast group member port aging time: When a port joins an IP multicast group, the aging timer of the port will begin timing. The multicast group member port aging time is set on this aging timer. If the switch has not received any IGMP report message before the timer times out, it transmits IGMP specific query message to the port.
- Maximum response time: When the switch transmits IGMP specific query message to the multicast member port, the Ethernet switch starts a response timer,

which times before the response to the query. If the switch has not received any IGMP report message before the timer times out, it will remove the port from the multicast member ports

II. Implement Layer 2 multicast with IGMP Snooping

The Ethernet switch runs IGMP Snooping to listen to the IGMP messages and map the host and its ports to the corresponding multicast group address. To implement IGMP Snooping, the Layer 2 Ethernet switch processes different IGMP messages in the way illustrated in the figure below:

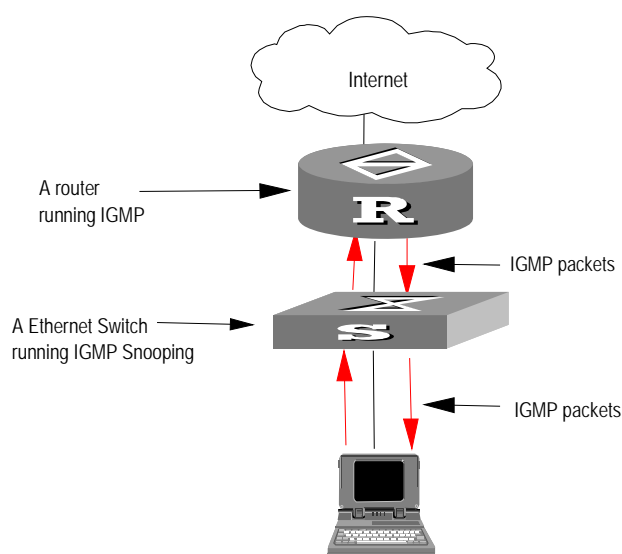


Figure 2-3 Implement IGMP Snooping

- 1) IGMP general query message: Transmitted by the multicast router to the multicast group members to query which multicast group contains member. When an IGMP general query message arrives at a router port, the Ethernet switch will reset the aging timer of the port. When a port other than a router port receives the IGMP general query message, the Ethernet switch will notify the multicast router that a port is ready to join a multicast group and starts the aging timer for the port.
- 2) IGMP specific query message: Transmitted from the multicast router to the multicast members and used for querying if a specific group contains any member. When received IGMP specific query message, the switch only transmits the specific query message to the IP multicast group which is queried.
- 3) IGMP report message: Transmitted from the host to the multicast router and used for applying to a multicast group or responding to the IGMP query message. When received the IGMP report message, the switch checks if the MAC multicast group corresponding to the IP multicast group the packet is ready to join exists. If the corresponding MAC multicast group does not exist, the switch only notifies the router that a member is ready to join a multicast group, creates a new MAC

multicast group, adds the port received the message to the group, starts the port aging timer, and then adds all the router ports in the native VLAN of the port into the MAC multicast forwarding table, and meanwhile creates an IP multicast group and adds the port received the report message to it. If the corresponding MAC multicast group exists but does not contains the port received the report message, the switch adds the port into the multicast group and starts the port aging timer. And then the switch checks if the corresponding IP multicast group exists. If it does not exist, the switch creates a new IP multicast group and adds the port received the report message to it. If it exists, the switch adds the port to it. If the MAC multicast group corresponding to the message exists and contains the port received the message, the switch will only reset the aging timer of the port.

- 4) IGMP leave message: Transmitted from the multicast group member to the multicast router to notify that a router host left the multicast group. When received a leave message of an IP multicast group, the Ethernet switch transmits the specific query message concerning that group to the port received the message, in order to check if the host still has some other member of this group and meanwhile starts a maximum response timer. If the switch has not receive any report message from the multicast group, the port will be removed from the corresponding MAC multicast group. If the MAC multicast group does not have any member, the switch will notify the multicast router to remove it from the multicast tree.

2.2 IGMP Snooping Configuration

The main IGMP Snooping configuration includes:

- Enabling/disabling IGMP Snooping
- Configuring the aging time of router port
- Configuring maximum response time
- Configuring the aging time of multicast group member port

Among the above configuration tasks, enabling IGMP Snooping is required, while others are optional for your requirements.

2.2.1 Enabling/Disabling IGMP Snooping

You can use the following commands to enable/disable IGMP Snooping to control whether MAC multicast forwarding table is created and maintained on Layer 2. First enable IGMP Snooping globally in system view, and then enable IGMP Snooping of the corresponding VLAN in VLAN view. The second step must be based on the first one.

Perform the following configuration in system view and VLAN view.

Table 2-1 Enabling/Disabling IGMP Snooping

Operation	Command
Enable/disable IGMP Snooping	igmp-snooping { enable disable }



Caution:

- Although layer 2 and layer 3 multicast protocols can run together, they cannot run on the same VLAN or its corresponding VLAN interface at the same time. For example, if the layer 2 multicast protocol is enabled on a VLAN, then the layer 3 multicast protocol cannot operate on this VLAN, and vice versa.
- IGMP Snooping functions only when it is enabled both in system view and in VLAN view.

By default, IGMP Snooping is disabled.

2.2.2 Configuring Router Port Aging Time

This task is to manually configure the router port aging time. If the switch has not received any general query message from the router before the router port is aged, it will remove the port from all the MAC multicast group.

Perform the following configuration in system view.

Table 2-2 Configuring router port aging time

Operation	Command
Configure router port aging time	igmp-snooping router-aging-time <i>seconds</i>
Restore the default aging time	undo igmp-snooping router-aging-time

By default, the port aging time is 105s.

2.2.3 Configuring Maximum Response Time

This task is to manually configure the maximum response time. If the Ethernet switch receives no report message from a port in the maximum response time, it will remove the port from the multicast group.

Perform the following configuration in system view.

Table 2-3 Configuring the maximum response time

Operation	Command
Configure the maximum response time	igmp-snooping max-response-time <i>seconds</i>
Restore the default setting	undo igmp-snooping max-response-time

By default, the maximum response time is 10 seconds.

2.2.4 Configuring Aging Time of Multicast Group Member

This task is to manually set the aging time of the multicast group member port. If the switch receives no multicast group report message during the member port aging time, it will transmit the specific query message to that port and starts a maximum response timer.

Perform the following configuration in system view.

Table 2-4 Configuring aging time of the multicast member

Operation	Command
Configure aging time of the multicast member	igmp-snooping host-aging-time <i>seconds</i>
Restore the default setting	undo igmp-snooping host-aging-time

By default, the aging time of the multicast member is 260 seconds.

2.3 Displaying and debugging IGMP Snooping

After the above configuration, execute **display** command in any view to display the running of the IGMP Snooping configuration, and to verify the effect of the configuration. Execute **reset** command in user view to reset the IGMP Snooping statistic information. Execute **debugging** command in user view to debug IGMP Snooping configuration.

Table 2-5 Displaying and debugging IGMP Snooping

Operation	Command
Display the information about current IGMP Snooping configuration	display igmp-snooping configuration
Display IGMP Snooping statistics of received and sent messages	display igmp-snooping statistics

Display IP/MAC multicast group information in the VLAN	display igmp-snooping group [vlan <i>vlanid</i>]
Reset the IGMP Snooping statistic information	reset igmp-snooping statistics

2.4 IGMP Snooping Configuration Example

2.4.1 Enable IGMP Snooping

I. Networking requirements

To implement IGMP Snooping on the switch, first enable it. The switch is connected with the router via the router port, and with user PC through the non-router ports in vlan 10.

II. Networking diagram

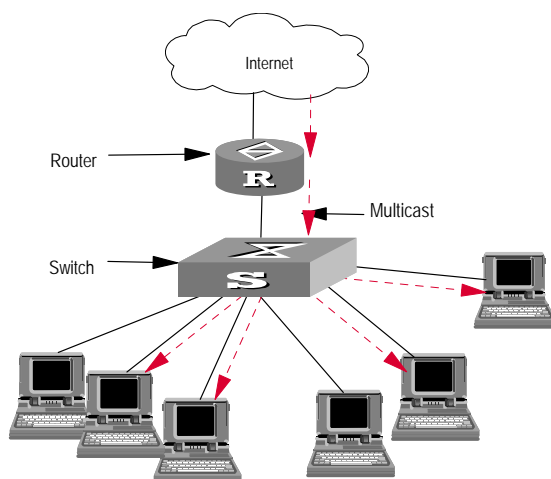


Figure 2-4 IGMP Snooping configuration networking

III. Configuration procedure

Enable IGMP Snooping globally.

```
[Quidway] igmp-snooping enable
```

Enable IGMP Snooping on VLAN 10.

```
[Quidway] vlan 10
```

```
[Quidway-vlan10] igmp-snooping enable
```

2.5 IGMP Snooping Fault Diagnosis and Troubleshooting

Fault: Multicast function cannot be implemented on the switch.

Troubleshooting:

- 1) IGMP Snooping is disabled.
 - Input the **display current-configuration** command to display the status of IGMP Snooping.
 - If the switch disabled IGMP Snooping, check whether the IGMP Snooping is not enabled globally or it is not enabled in the VLAN. If it is not enabled globally, first input the **igmp-snooping enable** command in system view and then in VLAN view. If it is not enabled in the VLAN, input the same command in VLAN view.
- 2) Multicast forwarding table set up by IGMP Snooping is wrong.
 - Input the **display igmp-snooping group** command to display if the multicast group is the expected one.
 - If the multicast group created by IGMP Snooping is not correct, turn to professional maintenance personnel for help.
 - Continue with diagnosis 3 if the second step is completed.
- 3) Multicast forwarding table set up on the bottom layer is wrong.
 - Enable IGMP Snooping group in user view and then input the command **display igmp-snooping group** to check if MAC multicast forwarding table in the bottom layer and that created by IGMP Snooping is consistent. You may also input the **display mac vlan** command in any view to check if MAC multicast forwarding table under vlanid in the bottom layer and that created by IGMP Snooping is consistent.
 - If they are not consistent, please contact the maintenance personnel for help.

Chapter 3 Common Multicast Configuration

3.1 Introduction to Common Multicast Configuration

The multicast common configuration is for both the multicast group management protocol and the multicast routing protocol. The configuration include enabling multicast, configuring multicast forwarding boundary and displaying multicast routing table and multicast forwarding table, etc.

3.2 Common Multicast Configuration

Common multicast configuration includes:

- Enabling multicast
- Configuring multicast route limit
- Clearing MFC forwarding entries or its statistic information
- Clearing route entries from the core multicast routing table

3.2.1 Enabling Multicast

Enable multicast first before enabling IGMP and the multicast routing protocol.

Perform the following configuration in system view.

Table 3-1 Enabling multicast

Operation	Command
Enable multicast	multicast routing-enable
Disable multicast	undo multicast routing-enable

By default, multicast is disabled.



Caution:

Only when multicast is enabled can other multicast configuration become effective.

3.2.2 Configuring Number Limit of Multicast Routing Entries

The number of multicast routing entries can be limited to prevent the router memory from being exhausted.

Please perform the following configurations in system view.

Table 3-2 Configuring number limit of multicast routing entries

Operation	Command
Configure number limit of multicast routing entries	multicast route-limit <i>limit</i>
Restore the default number limit	undo multicast route-limit

By default, the number limit of multicast routing entries is the maximum value permitted by the system, which differs by the types of routers.

3.2.3 Clearing MFC Forwarding Entries or Its Statistic Information

You can clear MFC forward entries or statistic information of MFC forward entries via the following command..

Perform the following configuration in user view.

Table 3-3 Clearing MFC forwarding entries or its statistic information

Operation	Command
Clear MFC forwarding entries or its statistic information	reset multicast forwarding-table [statistics] { all { <i>group-address</i> [mask { <i>group-mask</i> <i>group-mask-length</i> }] <i>source-address</i> [mask { <i>source-mask</i> <i>source-mask-length</i> }] incoming-interface Vlan-interface <i>vlan-interface-number</i> } * }

3.2.4 Clearing Route Entries From the Core Multicast Routing Table

You can clear route entries from the core multicast routing table, as well as MFC forwarding entries via the following command.

Perform the following configuration in user view.

Table 3-4 Clearing routing entries of multicast routing table

Operation	Command
Clear routing entries of multicast routing table	reset multicast routing-table { all { <i>group-address</i> [mask { <i>group-mask</i> <i>group-mask-length</i> }] <i>source-address</i> [mask { <i>source-mask</i> <i>source-mask-length</i> }] { incoming-interface Vlan-interface <i>vlan-interface-number</i> } } * }

The forwarding entries in MFC are deleted along with the routing entries in the multicast kernel routing table.

3.3 Displaying and debugging Common Multicast Configuration

After the above configuration, execute **display** command in any view to display the running of the multicast configuration, and to verify the effect of the configuration.

Execute **debugging** command in user view for the debugging of multicast.

Table 3-5 Displaying and debugging Common Multicast Configuration

Operation	Command
Display the multicast routing table	display multicast routing-table [<i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }] <i>source-address</i> [mask { <i>mask</i> <i>mask-length</i> }] incoming-interface { Vlan-interface <i>vlan-interface-number</i> register }]*
Display the multicast forwarding table	display multicast forwarding-table [<i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }] <i>source-address</i> [mask { <i>mask</i> <i>mask-length</i> }] incoming-interface { Vlan-interface <i>vlan-interface-number</i> register }]*
Enable multicast packet forwarding debugging	debugging multicast forwarding
Disable multicast packet forwarding debugging	undo debugging multicast forwarding
Enable multicast forwarding status debugging	debugging multicast status-forwarding
Disable multicast forwarding status debugging	undo debugging multicast status-forwarding
Enable multicast kernel routing debugging	debugging multicast kernel-routing

Disable multicast kernel routing debugging	undo debugging multicast kernel-routing
--	--

There are three types of multicast routing tables: individual multicast routing tables of each multicast routing protocol; a multicast kernel routing table integrating the routing information of those individual routing tables; and a multicast forwarding table in conformity with the kernel routing table and in charge of the multicast packet forwarding.

Multicast forwarding table is mainly used in debugging. Generally, users can obtain required information by viewing multicast kernel routing table.

Chapter 4 IGMP Configuration

4.1 IGMP Overview

IGMP (Internet Group Management Protocol) is a protocol in the TCP/IP suite responsible for management of IP multicast members. It is used to establish and maintain multicast membership among IP hosts and their directly connected neighboring routers. IGMP excludes transmitting and maintenance of membership information among multicast routers, which are completed by multicast routing protocols. All hosts participating in multicast must implement IGMP.

Hosts participating in IP multicast can join and leave a multicast group at any time. The number of members of a multicast group can be any integer and the location of them can be anywhere. A multicast router does not need and cannot keep the membership of all hosts. It only uses IGMP to learn whether receivers (i.e., group members) of a multicast group are present on the subnet connected to each interface. A host only needs to keep which multicast groups it has joined.

IGMP is not symmetric on hosts and routers. Hosts need to respond to IGMP query messages from the multicast router, i.e., report the group membership to the router. The router needs to send membership query messages periodically to discover whether hosts join the specified group on its subnets according to the received response messages. When the router receives the leave message, the router will send a group-specific query (IGMP Version 2) to discover whether no member exists in the group.

Up to now, IGMP has three versions, namely, IGMP Version 1 (defined by RFC1112), IGMP Version 2 (defined by RFC2236) and IGMP Version 3. At present, IGMP Version 2 is the most widely used version.

IGMP Version 2 boasts the following improvements over IGMP Version 1:

I. Election mechanism of multicast routers on the shared network segment

A shared network segment means that there are multiple multicast routers on a network segment. In this case, all routers running IGMP on the network segment can receive the membership report from hosts. Therefore, only one router is necessary to send membership query messages. In this case, the router election mechanism is required to specify a router as the querier.

In IGMP Version 1, selection of the querier is determined by the multicast routing protocol. While IGMP Version 2 specifies that the multicast router with the lowest IP

address is elected as the querier when there are multiple multicast routers on the same network segment.

II. Leaving group mechanism

In IGMP Version 1, hosts leave the multicast group quietly without informing the multicast router. In this case, the multicast router can only depend on the timeout of the response time of the multicast group to confirm that hosts leave the group. In Version 2, when a host is intended to leave, it will send a leave group message if it is the host who responds to the latest membership query message.

III. Specific group query

In IGMP Version 1, a query of a multicast router is targeted at all the multicast groups on the network segment, which is known as General Query.

In IGMP Version 2, Group-Specific Query is added besides general query. The destination IP address of the query packet is the IP address of the multicast group. The group address domain in the packet is also the IP address of the multicast group. This prevents the hosts of members of other multicast groups from sending response messages.

IV. Max response time

The Max Response Time is added in IGMP Version 2. It is used to dynamically adjust the allowed maximum time for a host to response to the membership query message.

4.2 Introduction to IGMP Proxy

A lot of leaf networks (leaf domains) are involved in the application of a multicast routing protocol (PIM-DM for example) over a large-scaled network. It is a hard work to configure and manage these leaf networks.

To reduce the configuration and management work without affecting the multicast connection of leaf networks, you can configure an IGMP Proxy in a leaf network switch (Switch B in the figure). The switch will then forward IGMP join or IGMP leave messages sent by the connected hosts. After the configuration of IGMP Proxy, the leaf switch is no longer a PIM neighbor but a host for the exterior network. Only when the switch has directly connected members, can it receive the multicast data of associated group.

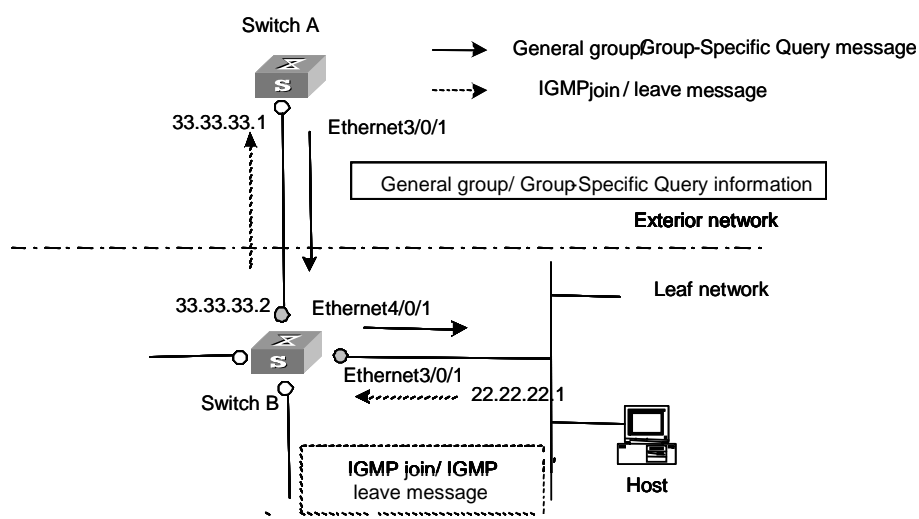


Figure 4-1 IGMP Proxy diagram

Figure 4-1 is an IGMP Proxy diagram for a leaf network.

First of all, configure PIM on Ethernet3/0/1 and Ethernet4/0/1 of Switch B. Then on Ethernet3/0/1 configure Ethernet4/0/1 as the outbound IGMP proxy interface of Ethernet4/0/1 to external networks (by configuring the **igmp proxy** command).

Then configure **pim neighbor-policy** on Ethernet3/0/1 interface of Switch A to filter PIM neighbors on network segment 33.33.33.0/24. That is, Switch A does not consider Switch B as its PIM neighbor.

In this case, when Switch B of leaf network receives from Ethernet3/0/1 interface an IGMP join or IGMP leave message sent by the host, it will change the source address of the IGMP information to the outbound interface address to Switch A (Ethernet 4/0/1 interface address: 33.33.33.2) and send the information to Ethernet3/0/1 interface of Switch A. This works as if there is a host directed connected to Ethernet 3/0/1 interface of Switch A. Similarly, when Switch B receives the general group or group-specific query message from Switch A, it will also change the source address of the query message to the outbound interface address of the host (Ethernet3/0/1 interface address: 22.22.22.1) and send the information from Ethernet3/0/1 interface.

In Figure 4-1, Ethernet3/0/1 interface of Switch B is called the client and Ethernet4/0/1 interface of Switch B is called the proxy.

4.3 IGMP Configuration

- 1) IGMP basic configuration includes:
 - Enabling multicast
 - Enabling IGMP on an interface
- 2) IGMP advanced configuration includes:

- Configuring the IGMP version
- Configuring the interval of sending IGMP Group-Specific Query packet
- Configuring the times of sending IGMP Group-Specific Query packet
- Configuring the limit of IGMP groups on an interface
- Configuring a router to join specified multicast group
- Controlling the access to IP multicast groups
- Configuring the IGMP query message interval
- Configuring the IGMP querier present timer
- Configuring the maximum query response time
- Deleting IGMP Groups Joined on an Interface

4.3.1 Enabling Multicast

Refer to “Common Multicast Configuration” of Chapter 3.

4.3.2 Enabling IGMP on an Interface

Only multicast function is enabled can the **igmp enable** command be executed. After this, you can initiate IGMP feature configuration.

Perform the following configuration in Interface view.

Table 4-1 Enabling/Disabling IGMP on an interface

Operation	Command
Enable IGMP on an interface	igmp enable
Disable IGMP on an interface	undo igmp enable

By default, IGMP is not enabled.

4.3.3 Configuring IGMP Proxy

IGMP proxy can be configured to reduce the configuration and management work of the leaf network without affecting the multicast connection there.

After IGMP proxy is configured on the leaf network Switch, the leaf switch acts as a host to the exterior network. Only when the switch has directly connected members, can it receive the multicast data of the associated group.

Perform the following configuration in interface view.

Table 4-2 Configuring IGMP proxy

Operation	Command
Specify the proxy interface of the current interface	igmp proxy Vlan-interface <i>vlan-interface-number</i>
Disable IGMP proxy of the interface	undo igmp proxy

By default, IGMP proxy is disabled.



Caution:

You must enable PIM on the interface before you configure the **igmp proxy** command. One interface can not be the IGMP proxy interface of two or more interfaces.

4.3.4 Configuring the IGMP Version

Perform the following configuration in Interface view.

Table 4-3 Selecting the IGMP version

Operation	Command
Select the IGMP version that the router uses	igmp version { 1 2 }
Restore the default setting	undo igmp version

By default, IGMP Version 2 is used.



Caution:

All routers on a subnet must support the same version of IGMP. After detecting the presence of IGMP Version 1 system, a router cannot automatically switch to Version 1.

4.3.5 Configuring the Interval for Querying IGMP Packets

The router finds out which multicast groups on its connected network segment have members by sending IGMP query messages periodically. Upon the reception of a response message, the router refreshes the membership information of the corresponding multicast group.

Please perform the following configurations in interface view.

Table 4-4 Configuring query interval

Operation	Command
Configure query interval	igmp timer query <i>seconds</i>
Restore the default query interval	undo igmp timer query

When there are multiple multicast routers on a network segment, the querier is responsible for sending IGMP query messages to all the hosts on the LAN.

By default, the interval is 60 seconds.

4.3.6 Configuring the Interval and the Number of Querying IGMP Packets

On the shared network, it is the query router (querier) that maintains IGMP membership on the interface. When an IGMP querier receives an IGMP Leave Group message from a host, the last member query interval can be specified for Group-Specific Queries.

- The host sends the IGMP Leave message.
- Upon receiving the message, IGMP querier sends the designated group IGMP query message for specified times (defined by the *robust-value* in **igmp robust-count**, with the default value as 2) and at a time interval (defined by the *seconds* in **igmp lastmember-queryinterval**, with the default value as 1 second).
- When other hosts receive the message from the IGMP querier and are interested in this group, they return the IGMP Membership Report message within the defined maximum response time.
- If IGMP querier receives the report messages from other hosts within the period equal to $robust-value \times seconds$, it continues membership maintenance for this group.
- If it receives no report message from any other host within this period, it reckons this as timeout and ends membership maintenance for this group.

This command can be used only when the querier runs IGMP version 2, since a host running IGMP Version 1 does not send IGMP Leave Group message when it leaves a group.

Please perform the following configurations in interface view.

I. Configuring interval for querying IGMP packets

Table 4-5 Configuring interval for querying IGMP packets

Operation	Command
Configure interval for querying IGMP packets	igmp lastmember-queryinterval <i>seconds</i>
Restore te default query interval	undo igmp lastmember-queryinterval

By default, the interval is 1 second.

II. Configuring the number of last member querying

Table 4-6 Configure the number of last member querying

Operation	Command
Configure number of last member querying	igmp robust-count <i>robust-value</i>
Restore the default number of querying	undo igmp robust-count

By default, an IGMP group-specific query message is sent for twice.

4.3.7 Configuring the limit of IGMP groups on an interface

If there is no limit to the number of IGMP groups added on a router interface or a router, the router memory may be exhausted, which may cause router failure.

You can set number limit for the IGMP groups added on the interface, but not the number limit for the IGMP groups added in the router, which is defined by the system.

Perform the following configuration in Interface view.

Table 4-7 Configuring the limit of IGMP groups on an interface

Operation	Command
Configure the limit of IGMP groups on an interface	igmp group-limit <i>limit</i>
Restore the limit of IGMP groups on an interface to the default value	undo igmp group-limit

By default, the maximum number of IGMP groups on an interface is 256.

If the number of IGMP groups on an interface has exceeded the specified value during configuration, no IGMP group will be deleted.

4.3.8 Configuring a Router to Join Specified Multicast Group

Usually, the host operating IGMP will respond to IGMP query packet of the multicast router. In case of response failure, the multicast router will consider that there is no multicast member on this network segment and will cancel the corresponding path. Configuring one interface of the router as multicast member can avoid such problem. When the interface receives IGMP query packet, the router will respond, thus ensuring that the network segment where the interface is connected can normally receive multicast packets.

For an ethernet switch, you can configure a port in a VLAN interface to join a multicast group.

Perform the following configuration in corresponding view.

Table 4-8 Configuring a router to join specified multicast group

Operation	Command
Configure a router to join specified multicast group (VLAN interface view)	igmp host-join <i>group-address</i> port { <i>interface_type</i> <i>interface_num</i> <i>interface_name</i> } [to { <i>interface_type</i> <i>interface_num</i> <i>interface_name</i> }]
Quit from specified multicast group (VLAN interface view)	undo igmp host-join <i>group-address</i> port { <i>interface_type</i> <i>interface_num</i> <i>interface_name</i> } [to { <i>interface_type</i> <i>interface_num</i> <i>interface_name</i> }]
Configure a router to join specified multicast group (Ethernet port view)	igmp host-join <i>group-address</i> vlan <i>vlanid</i>
Quit from specified multicast group (Ethernet port view)	undo igmp host-join <i>group-address</i> vlan <i>vlanid</i>

By default, a router joins no multicast group.

4.3.9 Limiting Multicast Groups An Interface Can Access

A multicast router learns whether there are members of a multicast group on the network via the received IGMP membership message. A filter can be set on an interface so as to limit the range of allowed multicast groups.

Perform the following configuration in corresponding view.

Table 4-9 Limiting multicast groups an interface can access

Operation	Command
Limit the range of allowed multicast groups on current interface (Interface view)	igmp group-policy <i>acl-number</i> [1 2 port { <i>interface_type</i> <i>interface_num</i> <i>interface_name</i> } [to { <i>interface_type</i> <i>interface_num</i> <i>interface_name</i> }]]
Remove the filter set on the interface (Interface view)	undo igmp group-policy [port { <i>interface_type</i> <i>interface_num</i> <i>interface_name</i> } [to { <i>interface_type</i> <i>interface_num</i> <i>interface_name</i> }]]

By default, no filter is configured, that is, all multicast groups are allowed on the interface.

4.3.10 Configuring the Interval to Send IGMP Query Message

Multicast routers send IGMP query messages to discover which multicast groups are present on attached networks. Multicast routers send query messages periodically to refresh their knowledge of members present on their networks.

Perform the following configuration in Interface view.

Table 4-10 Configuring the interval to send IGMP query message

Operation	Command
Configure the interval to send IGMP query message	igmp timer query <i>seconds</i>
Restore the default value	undo igmp timer query

When there are multiple multicast routers on a network segment, the querier is responsible for sending IGMP query messages to all hosts on the LAN.

By default, the interval is 60 seconds.

4.3.11 Configuring the Present Time of IGMP Querier

The IGMP querier present timer defines the period of time before the router takes over as the querier sending query messages, after the previous querier has stopped doing so.

Perform the following configuration in Interface view.

Table 4-11 Configuring the present time of IGMP querier

Operation	Command
Change the present time of IGMP querier	igmp timer other-querier-present <i>seconds</i>
Restore the default value	undo igmp timer other-querier-present

By default, the value is 120 seconds. If the router has received no query message within twice the interval specified by the **igmp timer query** command, it will regard the previous querier invalid.

4.3.12 Configuring Maximum Response Time for IGMP Query Message

Received a query message from a router, the host will set a timer for each multicast group it belongs to. The value of the timer is randomly selected between 0 and the maximum response time. When any timer becomes 0, the host will send the membership report message of the multicast group.

Setting the maximum response time reasonably can enable the host to respond to query messages quickly. In this case, the router can fast master the existing status of the members of the multicast group.

Perform the following configuration in Interface view.

Table 4-12 Configuring the maximum response time for IGMP query message

Operation	Command
Configure the maximum response time for IGMP query message	igmp max-response-time <i>seconds</i>
Restore the maximum query response time to the default value	undo igmp max-response-time

The smaller the maximum query response time value, the faster the router prunes groups. The actual response time is a random value in the range from 1 to 25 seconds. By default, the maximum query response time is 10 seconds.

4.3.13 Deleting IGMP Groups Joined on an Interface

You can delete an existing IGMP group from the interface via the following command.

Perform the following configuration in Interface view.

Table 4-13 Deleting IGMP groups joined on an interface

Operation	Command
Delete IGMP groups joined on an interface	reset igmp group { all interface Vlan-interface <i>vlan-interface-number</i> { all group-address [group-mask] } }

4.4 Displaying and debugging IGMP

After the above configuration, execute **display** command in any view to display the running of IGMP configuration, and to verify the effect of the configuration.

Execute **debugging** command in user view for the debugging of IGMP.

Table 4-14 Displaying and debugging IGMP

Operation	Command
Display the information about members of IGMP multicast groups	display igmp group [group-address interface Vlan-interface <i>vlan-interface-number</i>]
Display the IGMP configuration and running information about the interface	display igmp interface [Vlan-interface <i>vlan-interface-number</i>]
Enable the IGMP information debugging	debugging igmp { all event host packet timer }
Disable the IGMP information debugging	undo debugging igmp { all event host packet timer }

Chapter 5 PIM-DM Configuration

5.1 PIM-DM Overview

PIM-DM (Protocol Independent Multicast, Dense Mode) belongs to dense mode multicast routing protocols. PIM-DM is suitable for small networks. Members of multicast groups are relatively dense in such network environments.

The working procedures of PIM-DM include neighbor discovery, flood & prune and graft.

I. Neighbor discovery

The PIM-DM router needs to use Hello messages to perform neighbor discovery when it is started. All network nodes running PIM-DM keep in touch with one another with Hello messages, which are sent periodically.

II. Flood&Prune

PIM-DM assumes that all hosts on the network are ready to receive multicast data. When a multicast source "S" begins to send data to a multicast group "G", after the router receives the multicast packets, the router will perform RPF check according to the unicast routing table first. If the RPF check is passed, the router will create an (S, G) entry and then flood the data to all downstream PIM-DM nodes. If the RPF check is not passed, that is, multicast packets enter from an error interface, the packets will be discarded. After this process, an (S, G) entry will be created in the PIM-DM multicast domain.

If the downstream node has no multicast group members, it will send a Prune message to the upstream nodes to inform the upstream node not to forward data to the downstream node. Receiving the prune message, the upstream node will remove the corresponding interface from the outgoing interface list corresponding to the multicast forwarding entry (S, G). In this way, a SPT (Shortest Path Tree) rooted at Source S is built. The pruning process is initiated by leaf routers first.

This process is called "flood & prune" process. In addition, nodes that are pruned provide timeout mechanism. Each router re-starts the "flood & prune" process upon pruning timeout. The consistent "flood & prune" process of PIM-DM is performed periodically.

During this process, PIM-DM uses the RPF check and the existing unicast routing table to build a multicast forwarding tree rooted at the data source. When a packet arrives,

the router will first judge the correctness of the path. If the interface that the packet arrives is the one indicated by the unicast routing to the multicast source, the packet is regarded to be from the correct path. Otherwise, the packet will be discarded as a redundancy packet without the multicast forwarding. The unicast routing information as path judgment can come from any unicast routing protocol independent of any specified unicast routing protocol such as the routing information learned by RIP and OSPF

III. Assert mechanism

As shown in the following figure, both routers A and B on the LAN have their own receiving paths to multicast source S. In this case, when they receive a multicast packet sent from multicast source S, they will both forward the packet to the LAN. Multicast Router C at the downstream node will receive two copies of the same multicast packet.

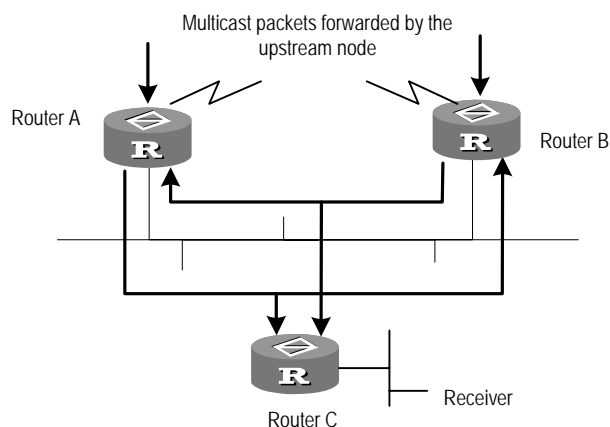


Figure 5-1 Assert mechanism diagram

When they detect such a case, routers need to select a unique sender by using the assert mechanism. Routers will send Assert packets to select the best path. If two or more than two paths have the same priority and metric, the path with a higher IP address will be the upstream neighbor of the (S, G) entry, which is responsible for forwarding the (S, G) multicast packet.

IV. Graft

When the pruned downstream node needs to be restored to the forwarding state, the node will send a graft packet to inform the upstream node.

5.2 PIM-DM Configuration

- 1) PIM-DM basic configuration includes:
 - Enabling multicast

- Enabling PIM-DM
- 2) PIM-DM advanced configuration includes:
 - Configuring Sending Interval for the Hello Packets
 - Entering the PIM view
 - Configuring filtering of multicast source/group
 - Configuring filtering of PIM neighbor
 - Configuring the maximum number of PIM neighbor on an interface
 - Clearing multicast route entries from PIM routing table
 - Clearing PIM neighbor

When the router is run in the PIM-DM domain, it is recommended to enable PIM-DM on all interfaces of the non-border router.

5.2.1 Enabling Multicast

Refer to “Common Multicast Configuration” of Chapter 3.

5.2.2 Enabling PIM-DM

PIM-DM needs to be enabled in configuration of all interfaces.

After PIM-DM is enabled on an interface, it will send PIM Hello messages periodically and process protocol packets sent by PIM neighbors.

Perform the following configuration in Interface view.

Table 5-1 Enabling PIM-DM

Operation	Command
Enable PIM-DM on an interface	pim dm
Disable PIM-DM on an interface	undo pim dm

It's recommended to configure PIM-DM on all interfaces in non-special cases. This configuration is effective only after the multicast routing is enabled in system view.

Once enabled PIM-DM on an interface, PIM-SM cannot be enabled on the same interface and vice versa.

5.2.3 Entering the PIM View

Global parameters of PIM should be configured in PIM view.

Perform the following configuration in system view.

Table 5-2 Entering PIM view

Operation	Command
Enter PIM view	pim
Back to system view	undo pim

Using **undo pim** command, you can clear the configuration in PIM view, and back to system view.

5.2.4 Configuring Sending Interval for the Hello Packets

After PIM is enabled on an interface, it will send Hello messages periodically on the interface. The interval at which Hello messages are sent can be modified according to the bandwidth and type of the network connected to the interface.

Perform the following configuration in Interface view.

Table 5-3 Configuring hello message interval on an interface

Operation	Command
Configure the hello message interval on an interface	pim timer hello <i>seconds</i>
Restore the interval to the default value	undo pim timer hello

The default interval is 30 seconds. You can configure the value according to different network environments. Generally, this parameter does not need to be modified.

This configuration can be performed only after PIM (PIM-DM or PIM-SM) is enabled in Interface view.

5.2.5 Configuring the Filtering of Multicast Source/Group

You can set to filter the source (and group) address of multicast data packets via this command. When this feature is configured, the router filters not only multicast data, but the multicast data encapsulated in the registration packets.

Perform the following configuration in the PIM view.

Table 5-4 Configuring the filtering of multicast source/group

Operation	Command
Configure the filtering of multicast source/group	source-policy <i>acl-number</i>

Remove the configuration of filtering	undo source-policy
---------------------------------------	---------------------------

If source address filtering is configured, as well as basic ACLs, then the router filters the source addresses of all multicast data packets received. Those not matched will be discarded.

If source address filtering is configured, as well as advanced ACLs, then the router filters the source and group addresses of all multicast data packets received. Those not matched will be discarded.

5.2.6 Configuring the Filtering of PIM Neighbor

You can set to filter the PIM neighbors on the current interface via the following configuration.

Perform the following configuration in the PIM view.

Table 5-5 Configuring the filtering of PIM neighbor

Operation	Command
Configure filtering of PIM neighbor	pim neighbor-policy <i>acl-number</i>
Remove the configuration of filtering	undo pim neighbor-policy

By default, no filtering rules are set.

Only the routers that match the filtering rule in the ACL can serve as a PIM neighbor of the current interface.

5.2.7 Configuring the Maximum Number of PIM Neighbor on an Interface

The maximum number of PIM neighbors of a router interface can be configured to avoid exhausting the memory of the router or router faults. The maximum number of PIM neighbors of a router is defined by the system, and is not open for modification.

Perform the following configuration in the PIM view.

Table 5-6 Configuring the maximum number of PIM neighbor on an interface

Operation	Command
Configure the maximum number of PIM neighbor on an interface	pim neighbor-limit <i>limit</i>
Restore the limit of PIM neighbor to the default value	pim neighbor-limit

By default, the PIM neighbors on the interface are limited to 128.

If the number of PIM neighbors of an interface has exceeded the configured value by the time of configuration, the existing PIM neighbors will not be deleted.

5.2.8 Clearing multicast route entries from PIM routing table

Perform the following configuration in user view.

Table 5-7 Clearing multicast route entries from PIM routing table

Operation	Command
Clear multicast route entries from PIM routing table	reset pim routing-table { all { <i>group-address</i> [mask { <i>group-mask</i> <i>group-mask-length</i> }] <i>source-address</i> [mask { <i>source-mask</i> <i>source-mask-length</i> }] { incoming-interface { Vlan-interface <i>vlan-interface-number</i> null } } * }

If in this command, the *group-address* is 224.0.0.0/24 and *source-address* is the RP address (where group address can have a mask, but the resulted IP address must be 224.0.0.0, and source address has no mask), then it means only the (*, *, RP) item will be cleared.

If in this command, the *group-address* is any a group address, and *source-address* is 0 (where group address can have a mask, and source address has no mask), then only the (*, G) item will be cleared.

Note that this command shall clear not only multicast route entries from PIM routing table, but also the corresponding route entries and forward entries in the multicast core routing table and MFC.

5.2.9 Clearing PIM Neighbors

Perform the following configuration in user view.

Table 5-8 Reseting PIM neighbor

Operation	Command
Clear PIM neighbors	reset pim neighbor { all { <i>neighbor-address</i> interface Vlan-interface <i>vlan-interface-number</i> } * }

5.3 Displaying and debugging PIM-DM

After the above configuration, execute **display** command in any view to display the running of PIM-DM configuration, and to verify the effect of the configuration.

Execute **debugging** command in user view for the debugging of PIM-DM.

Table 5-9 Displaying and debugging PIM-DM

Operation	Command
Display the PIM multicast routing table	display pim routing-table [{ { *g [group-address [mask { mask-length mask }]] **rp [rp-address [mask { mask-length mask }]] } { group-address [mask { mask-length mask }] source-address [mask { mask-length mask }] } * } incoming-interface { Vlan-interface vlan-interface-number null } { dense-mode sparse-mode }] *
Display the PIM interface information	display pim interface [Vlan-interface vlan-interface-number]
Display the information about PIM neighboring routers	display pim neighbor [interface Vlan-interface vlan-interface-number]
Enable the PIM debugging	debugging pim common { all event packet timer }
Disable the PIM debugging	undo debugging pim common { all event packet timer }
Enable the PIM-DM debugging	debugging pim dm { alert all mbr mrt timer warning { recv send } { all assert graft graft-ack join prune } }
Disable the PIM-DM debugging	undo debugging pim dm { alert all mbr mrt timer warning { recv send } { all assert graft graft-ack join prune } }

5.4 PIM-DM Configuration Example

I. Networking requirements

A port of LS_A is added to Vlan 10 to connect Multicast Source; a port is added to Vlan11 to connect LS_B; a port is added to Vlan12 to connect LS_C. Configure to implement multicast between Multicast Source and Receiver 1 and Receiver 2.

II. Networking diagram

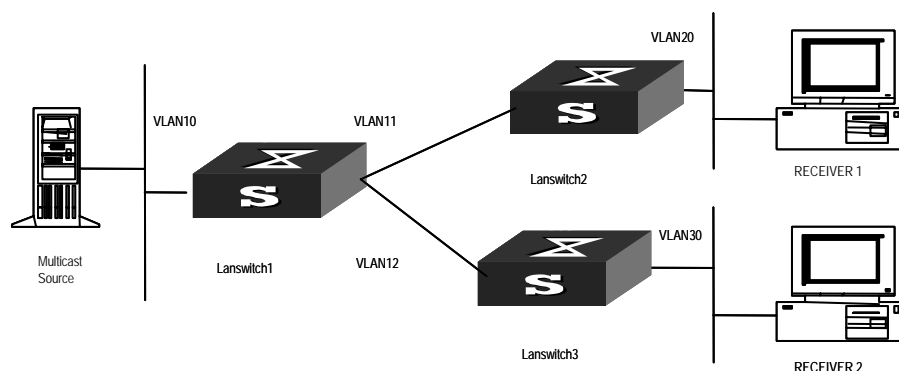


Figure 5-2 PIM-DM configuration networking

III. Configuration procedure

This section only introduces LS_A configuration procedure, while LS_B and LS_C configuration procedures are similar.

Enable the multicast routing protocol.

```
[Quidway] multicast routing-enable
```

Enable IGMP and PIM-DM.

```
[Quidway] vlan 10
```

```
[Quidway-vlan10] port ethernet 1/0/2 to ethernet 1/0/3
```

```
[Quidway-vlan10] quit
```

```
[Quidway] vlan 11
```

```
[Quidway-vlan11] port ethernet 1/0/4 to ethernet 1/0/5
```

```
[Quidway-vlan11] quit
```

```
[Quidway] vlan 12
```

```
[Quidway-vlan12] port ethernet 1/0/6 to ethernet 1/0/7
```

```
[Quidway-vlan12] quit
```

```
[Quidway] interface vlan-interface 10
```

```
[Quidway-vlan-interface10] ip address 1.1.1.1 255.255.0.0
```

```
[Quidway-vlan-interface10] igmp enable
```

```
[Quidway-vlan-interface10] pim dm
```

```
[Quidway-vlan-interface10] quit
```

```
[Quidway] interface vlan-interface 11
```

```
[Quidway-vlan-interface11] ip address 2.2.2.2 255.255.0.0
```

```
[Quidway-vlan-interface11] igmp enable
```

```
[Quidway-vlan-interface11] pim dm
```

```
[Quidway-vlan-interface11] quit
```

```
[Quidway] interface vlan-interface 12
```

```
[Quidway-vlan-interface12] ip address 3.3.3.3 255.255.0.0  
[Quidway-vlan-interface11] igmp enable  
[Quidway-vlan-interface12] pim dm
```

Chapter 6 PIM-SM Configuration

6.1 PIM-SM Overview

6.1.1 Introduction to PIM-SM

PIM-SM (Protocol Independent Multicast, Sparse Mode) belongs to sparse mode multicast routing protocols. PIM-SM is mainly applicable to large-scale networks with broad scope in which group members are relatively sparse.

Different from the flood & prune principle of the dense mode, PIM-SM assumes that all hosts do not need to receive multicast packets, unless there is an explicit request for the packets.

PIM-SM uses the RP (Rendezvous Point) and the BSR (Bootstrap Router) to advertise multicast information to all PIM-SM routers and uses the join/prune information of the router to build the RP-rooted shared tree (RPT), thereby reducing the bandwidth occupied by data packets and control packets and reducing the process overhead of the router. Multicast data flows along the shared tree to the network segments the multicast group members are on. When the data traffic is sufficient, the multicast data flow can switch over to the SPT (Shortest Path Tree) rooted on the source to reduce network delay. PIM-SM does not depend on the specified unicast routing protocol but uses the present unicast routing table to perform the RPF check.

Running PIM-SM needs to configure candidate RPs and BSRs. The BSR is responsible for collecting the information from the candidate RP and advertising the information.

6.1.2 PIM-SM Operating Principle

The PIM-SM working process is as follows: neighbor discovery, building the RP-rooted shared tree (RPT), multicast source registration and SPT switchover etc. The neighbor discovery mechanism is the same as that of PIM-DM, which will not be described any more.

I. Build the RP shared tree (RPT)

When hosts join a multicast group G, the leaf routers that directly connect with the hosts send IGMP messages to learn the receivers of multicast group G. In this way, the leaf routers calculate the corresponding rendezvous point (RP) for multicast group G and

then send join messages to the node of a higher level toward the rendezvous point (RP). Each router along the path between the leaf routers and the RP will generate (*, G) entries in the forwarding table, indicating that all packets sent to multicast group G are applicable to the entries no matter from which source they are sent. When the RP receives the packets sent to multicast group G, the packets will be sent to leaf routers along the path built and then reach the hosts. In this way, an RP-rooted tree (RPT) is built as shown in the following figure.

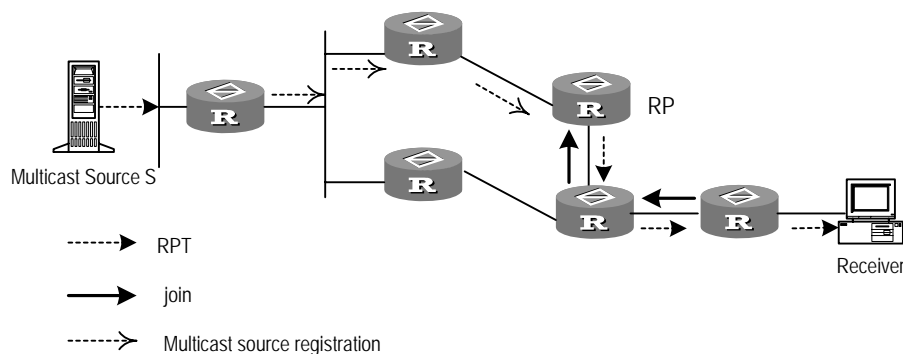


Figure 6-1 RPT schematic diagram

II. Multicast source registration

When multicast source S sends a multicast packet to the multicast group G, the PIM-SM multicast router directly connected to S will encapsulate the received packet into a registration packet and send it to the corresponding RP in unicast form. If there are multiple PIM-SM multicast routers on a network segment, the Designated Router (DR) will be responsible for sending the multicast packet.

6.1.3 Preparations before Configuring PIM-SM

I. Configuring candidate RPs

In a PIM-SM network, multiple RPs (candidate-RPs) can be configured. Each Candidate-RP (C-RP) is responsible for forwarding multicast packets with the destination addresses in a certain range. Configuring multiple C-RPs is to implement load balancing of the RP. These C-RPs are equal. All multicast routers calculate the RPs corresponding to multicast groups according to the same algorithm after receiving the C-RP messages that the BSR advertises.

It should be noted that one RP can serve multiple multicast groups or all multicast groups. Each multicast group can only be uniquely correspondent to one RP at a time rather than multiple RPs.

II. Configuring BSRs

The BSR is the management core in a PIM-SM network. Candidate-RPs send announcement to the BSR, which is responsible for collecting and advertising the information about all candidate-RPs.

It should be noted that there can be only one BSR in a network but you can configure multiple candidate-BSRs. In this case, once a BSR fails, you can switch over to another BSR. A BSR is elected among the C-BSRs automatically. The C-BSR with the highest priority is elected as the BSR. If the priority is the same, the C-BSR with the largest IP address is elected as the BSR.

III. Configuring static RP

The router that serves as the RP is the core router of multicast routes. If the dynamic RP elected by BSR mechanism is invalid for some reason, the static RP can be configured to specify RP. As the backup of dynamic RP, static RP improves network robusticity and enhances the operation and management capability of multicast network.

6.2 PIM-SM Configuration

- 1) PIM-SM basic configuration includes:
 - Enabling Multicast
 - Enabling PIM-SM
 - Entering the PIM view
 - Configuring the PIM-SM domain border
 - Configuring candidate-BSRs
 - Configuring candidate-RPs
 - Configuring static RP
- 2) PIM-SM advanced configuration includes:
 - Configuring the sending interval for the Hello packets of the interface
 - Configuring the filtering of multicast source/group
 - Configuring the filtering of PIM neighbor
 - Configuring the maximum number of PIM neighbor on an interface
 - Configuring RP to filter the register messages sent by DR
 - Limiting the range of legal BSR
 - Limiting the range of legal C-RP
 - Clearing multicast route entries from PIM routing table
 - Clearing PIM neighbor

It should be noted that at least one router in an entire PIM-SM domain should be configured with Candidate-RPs and Candidate-BSRs.

6.2.1 Enabling Multicast

Refer to “Common Multicast Configuration” of Chapter 3.

6.2.2 Enabling PIM-SM

This configuration can be effective only after multicast is enabled.

Perform the following configuration in Interface view.

Table 6-1 Enabling PIM-SM

Operation	Command
Enable PIM-SM on an interface	pim sm
Disable PIM-SM on an interface	undo pim sm

Repeat this configuration to enable PIM-SM on other interfaces. Only one multicast routing protocol can be enabled on an interface at a time.

Once enabled PIM-SM on an interface, PIM-DM cannot be enabled on the same interface and vice versa.

6.2.3 Configuring the PIM-SM Domain Border

After the PIM-SM domain border is configured, bootstrap messages cannot cross the border in any direction. In this way, the PIM-SM domain can be split.

Perform the following configuration in Interface view.

Table 6-2 Configuring the PIM-SM domain border

Operation	Command
Set the PIM-SM domain border	pim bsr-boundary
Remove the PIM-SM domain border configured	undo pim bsr-boundary

By default, no domain border is set. After this configuration is performed, a bootstrap message cannot cross the border but other PIM packets can. This configuration can effectively divide a network into domains using different BSRs.

6.2.4 Entering the PIM view

Global parameters of PIM should be configured in PIM view.

Perform the following configuration in system view.

Table 6-3 Entering the PIM view

Operation	Command
Enter the PIM view	pim
Back to system view	undo pim

Using **undo pim** command, you can clear the configuration in PIM view, and back to system view.

6.2.5 Configuring Candidate-BSRs

In a PIM domain, one or more candidate BSRs should be configured. A BSR (Bootstrap Router) is elected among candidate BSRs. The BSR takes charge of collecting and advertising RP information.

The automatic election among candidate BSRs is described as follows:

One interface which has started PIM-SM must be specified when configuring the router as the candidate BSR.

At first, each candidate BSR considers itself as the BSR of the PIM-SM domain, and sends Bootstrap message by taking the IP address of the interface as the BSR address.

When receiving Bootstrap messages from other routers, the candidate BSR will compare the BSR address of the newly received Bootstrap message with that of itself. Comparison standards include priority and IP address. The bigger IP address is considered better when the priority is the same. If the new BSR address is better, the candidate BSR will replace its BSR address and stop regarding itself as the BSR. Otherwise, the candidate BSR will keep its BSR address and continue to regard itself as the BSR.

Perform the following configuration in PIM view.

Table 6-4 Configuring candidate-BSRs

Operation	Command
Configure a candidate-BSR	c-bsr Vlan-interface <i>vlan-interface-number hash-mask-len</i> [<i>priority</i>]
Remove the candidate-BSR configured	undo c-bsr

Candidate-BSRs should be configured on the routers in the network backbone. By default, no BSR is set. The default priority is 0.



Caution:

One router can only be configured with one candidate-BSR. When a candidate-BSR is configured on another interface, it will replace the previous configuration.

6.2.6 Configuring Candidate-RPs

In PIM-SM, the shared tree built by the multicast routing data is rooted at the RP. There is a mapping from a multicast group to an RP. A multicast group can be mapped to an RP. Different groups can be mapped to one RP.

Perform the following configuration in PIM view.

Table 6-5 Configuring candidate-RPs

Operation	Command
Configure a candidate-RP	c-rp Vlan-interface <i>vlan-interface-number</i> [group-policy <i>acl-number</i> priority <i>priority-value</i>]*
Remove the candidate-RP configured	undo c-rp { Vlan-interface <i>vlan-interface-number</i> all }

When configuring RP, if the range of the served multicast group is not specified, the RP will serve all multicast groups. Otherwise, the range of the served multicast group is the multicast group in the specified range. It is suggested to configure Candidate RP on the backbone router.

6.2.7 Configuring Static RP

Static RP serves as the backup of dynamic RP, so as to improve network robusticity.

Perform the following configuration in PIM view.

Table 6-6 Configuring static RP

Operation	Command
Configure static RP	static-rp <i>rp-address</i> [<i>acl-number</i>]

Remove the configured static RP	undo static-rp <i>rp-address</i>
---------------------------------	---

Basic ACL can control the range of multicast group served by static RP.

If static RP is in use, all routers in the PIM domain must adopt the same configuration. If the configured static RP address is the interface address of the local router whose state is UP, the router will function as the static RP. It is unnecessary to enable PIM on the interface that functions as static RP.

When the RP elected from BSR mechanism is valid, static RP does not work.

6.2.8 Configuring the sending interval for the Hello packets of the interface

Generally, PIM-SM advertises Hello messages periodically on the interface enabled with it to detect PIM neighbors and discover which router is the Designated Router (DR).

Perform the following configuration in Interface view.

Table 6-7 Configuring the sending interval for the Hello packets of the interface

Operation	Command
Configure the sending interval for the Hello packets of the interface	pim timer hello <i>seconds</i>
Restore the interval to the default value	undo pim timer hello

By default, the hello message interval is 30 seconds. Users can configure the value according to different network environments.

This configuration can be performed only after the PIM (PIM-DM or PIM-SM) is enabled in Interface view.

6.2.9 Configuring the filtering of multicast source/group

Refer to “PIM-DM Configuration” of Chapter 5.

6.2.10 Configuring the filtering of PIM neighbor

Refer to “PIM-DM Configuration” of Chapter 5.

6.2.11 Configuring the maximum number of PIM neighbor on an interface

Refer to “PIM-DM Configuration” of Chapter 5.

6.2.12 Configuring RP to Filter the Register Messages Sent by DR

In the PIM-SM network, the register message filtering mechanism can control which sources to send messages to which groups on the RP, i.e., RP can filter the register messages sent by DR to accept specified messages only.

Perform the following configuration in PIM view.

Table 6-8 Configuring RP to filter the register messages sent by DR

Operation	Command
Configure RP to filter the register messages sent by DR	register-policy <i>acl-number</i>
Cancel the configured filter of messages	undo register-policy

If an entry of a source group is denied by the ACL, or the ACL does not define operation to it, or there is no ACL defined, the RP will send RegisterStop messages to the DR to prevent the register process of the multicast data stream.



Caution:

Only the register messages matching the ACL **permit** clause can be accepted by the RP. Specifying an undefined ACL will make the RP to deny all register messages.

6.2.13 Limiting the range of legal BSR

In the PIM SM network using BSR (bootstrap router) mechanism, every router can set itself as C-BSR (candidate BSR) and take the authority to advertise RP information in the network once it wins in the contention. To prevent malicious BSR proofing in the network, the following two measures need to be taken:

- Prevent the router from being spoofed by hosts though faking legal BSR messages to modify RP mapping. BSR messages are of multicast type and their TTL is 1, so this type of attacks often hit edge routers. Fortunately, BSRs are inside the network, while assaulting hosts are outside, therefore neighbor and RPF checks can be used to stop this type of attacks.
- If a router in the network is manipulated by an attacker, or an illegal router is accessed into the network, the attacker may set itself as C-BSR and try to win the contention and gain authority to advertise RP information among the network. Since the router configured as C-BSR shall propagate BSR messages, which are

multicast messages sent hop by hop with TTL as 1, among the network, then the network cannot be affected as long as the peer routers do not receive these BSR messages. One way is to configure **bsr-policy** on each router to limit legal BSR range, for example, only 1.1.1.1/32 and 1.1.1.2/32 can be BSR, thus the routers cannot receive or forward BSR messages other than these two. Even legal BSRs cannot contest with them.

Perform the following configuration in PIM view.

Table 6-9 Limiting the range of legal BSR

Operation	Command
Set the the limit legal BSR range	bsr-policy <i>acl-number</i>
Restore to the default setting	undo bsr-policy

For detailed information of **bsr-policy**, please refer to the command manual.

6.2.14 Limiting the range of legal C-RP

In the PIM SM network using BSR mechanism, every router can set itself as C-RP (candidate rendezvous point) servicing particular groups. If elected, a C-RP becomes the RP servicing the current group.

In BSR mechanism, a C-RP router unicasts C-RP messages to the BSR, which then propagates the C-RP messages among the network by BSR message. To prevent C-RP spoofing, you need to configure **crp-policy** on the BSR to limit legal C-RP range and their service group range. Since each C-BSR has the chance to become BSR, you must configure the same filtering policy on each C-BSR router.

Perform the following configuration in PIM view.

Table 6-10 Limiting the range of legal C-RP

Operation	Command
Set the the limit legal C-RP range	crp-policy <i>acl-number</i>
Restore to the default setting	undo crp-policy

For detailed information of **crp-policy**, please refer to the command manual.

6.2.15 Clearing multicast route entries from PIM routing table

Refer to “PIM-DM Configuration” of Chapter 5.

6.2.16 Clearing PIM Neighbors

Refer to “PIM-DM Configuration” of Chapter 5.

6.3 Displaying and debugging PIM-SM

After the above configuration, execute **display** command in any view to display the running of PIM-SM configuration, and to verify the effect of the configuration.

Execute **debugging** command in user view for the debugging of PIM-SM.

Table 6-11 Displaying and debugging PIM-SM

Operation	Command
Display the BSR information	display pim bsr-info
Display the RP information	display pim rp-info [<i>group-address</i>]
Enable the PIM-SM debugging	debugging pim sm { all verbose mrt warning mbr { alert fresh } timer { assert bsr crpadv jp jpgdelay mrt probe spt } { recv send } { assert bootstrap crpadv reg regstop jp } }
Disable the PIM-SM debugging	undo debugging pim sm { all verbose mrt warning mbr { alert fresh } timer { assert bsr crpadv jp jpgdelay mrt probe spt } { recv send } { assert bootstrap crpadv reg regstop jp } }

6.4 PIM-SM Configuration Example

I. Networking requirements

In actual network, we assume that the switches can intercommunicate.

Suppose that Host A is the receiver of the multicast group at 225.0.0.1. Host B begins transmitting data destined to 225.0.0.1. LS_A receives the multicast data from Host B via LS_B.

II. Networking diagram

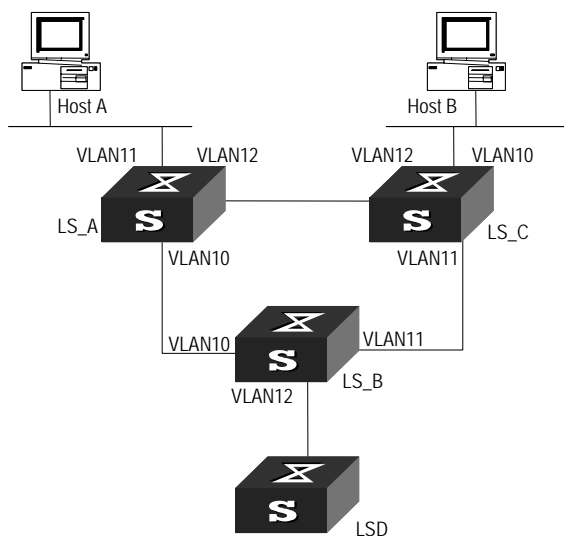


Figure 6-2 PIM-SM configuration networking

III. Configuration procedure

1) Configure LS_A

Enable PIM-SM.

```
[Quidway] multicast routing-enable
[Quidway] vlan 10
[Quidway-vlan10] port ethernet 1/0/2 to ethernet 1/0/3
[Quidway-vlan10] quit
[Quidway] interface vlan-interface 10
[Quidway-vlan-interface10] igmp enable
[Quidway-vlan-interface10] pim sm
[Quidway-vlan-interface10] quit
[Quidway] vlan 11
[Quidway-vlan11] port ethernet 1/0/4 to ethernet 1/0/5
[Quidway-vlan11] quit
[Quidway] interface vlan-interface 11
[Quidway-vlan-interface11] igmp enable
[Quidway-vlan-interface11] pim sm
[Quidway-vlan-interface11] quit
[Quidway] vlan 12
[Quidway-vlan12] port ethernet 1/0/6 to ethernet 1/0/7
[Quidway-vlan12] quit
[Quidway] interface vlan-interface 12
[Quidway-vlan-interface12] igmp enable
```

```
[Quidway-vlan-interface12] pim sm
[Quidway-vlan-interface12] quit
```

2) Configure LS_B

Enable PIM-SM.

```
[Quidway] multicast routing-enable
[Quidway] vlan 10
[Quidway-vlan10] port ethernet 1/0/2 to ethernet 1/0/3
[Quidway-vlan10] quit
[Quidway] interface vlan-interface 10
[Quidway-vlan-interface10] igmp enable
[Quidway-vlan-interface10] pim sm
[Quidway-vlan-interface10] quit
[Quidway] vlan 11
[Quidway-vlan11] port ethernet 1/0/4 to ethernet 1/0/5
[Quidway-vlan11] quit
[Quidway] interface vlan-interface 11
[Quidway-vlan-interface11] igmp enable
[Quidway-vlan-interface11] pim sm
[Quidway-vlan-interface11] quit
[Quidway] vlan 12
[Quidway-vlan12] port ethernet 1/0/6 to ethernet 1/0/7
[Quidway-vlan12] quit
[Quidway] interface vlan-interface 12
[Quidway-vlan-interface12] igmp enable
[Quidway-vlan-interface12] pim sm
[Quidway-vlan-interface12] quit
```

Configure the C-BSR.

```
[Quidway] pim
[Quidway-pim] c-bsr vlan-interface 10 30 2
```

Configure the C-RP.

```
[Quidway] acl number 2000
[Quidway-acl-basic-2000] rule permit source 225.0.0.0 0.255.255.255
[Quidway] pim
[Quidway-pim] c-rp vlan-interface 10 group-policy 2000
```

Configure PIM domain border.

```
[Quidway] interface vlan-interface 12
[Quidway-vlan-interface12] pim bsr-boundary
```

After VLAN-interface 12 is configured as domain border, the LS_D will be excluded from the local PIM domain and cannot receive the BSR information transmitted from LS_B any more.

3) Configure LS_C.

Enable PIM-SM.

```
[Quidway] multicast routing-enable
[Quidway] vlan 10
[Quidway-vlan10] port ethernet 1/0/2 to ethernet 1/0/3
[Quidway-vlan10] quit
[Quidway] interface vlan-interface 10
[Quidway-vlan-interface10] igmp enable
[Quidway-vlan-interface10] pim sm
[Quidway-vlan-interface10] quit
[Quidway] vlan 11
[Quidway-vlan11] port ethernet 1/0/4 to ethernet 1/0/5
[Quidway-vlan11] quit
[Quidway] interface vlan-interface 11
[Quidway-vlan-interface11] igmp enable
[Quidway-vlan-interface11] pim sm
[Quidway-vlan-interface11] quit
[Quidway] vlan 12
[Quidway-vlan12] port ethernet 1/0/6 to ethernet 1/0/7
[Quidway-vlan12] quit
[Quidway] interface vlan-interface 12
[Quidway-vlan-interface12] igmp enable
[Quidway-vlan-interface12] pim sm
[Quidway-vlan-interface12] quit
```