Multicast Configuration

Table of Contents

Chapter 1   **Multicast Overview**

The chapter describes how to cofigure the multicast routing protocol. For the details of the multicast routing commands, refer to the part "Multicast Routing Commands".

The traditional IP transmission allows only one host to communicate with a single host (unicast communication) or to communicate with all hosts (broadcast communication). The multicast technology allows one host to send message to some hosts. These hosts are called as group members.

The destination address of the message sent to the group member is a D-class address (224.0.0.0~239.255.255.255). The multicast message is transmitted like UDP. It does not provide reliable transmission and error control as TCP does.

The sender and the receiver make up of a multicast application. The sender can send the multicast message without joining in a group. However, the receiver has to join in a group before it receives the message from the group.

The relationship between group members is dynamic. The host can join in or leave a group at any time. There is no limitation to the location and number of the group member. If necessary, a host can be a member of multiple groups. Therefore, the state of the group and the number of group members varies with the time.

The router can maintain the routing table for forwarding multicast message by executing the multicast routing protocol such as PIM-DM and PIM-SM. The router learns the state of the group members in the directly-connected network segment through IGMP. The host can join in a designated IGMP group by sending the **IGMP Report** message.

The IP multicast technology is suitable for the one-to-multiple multimedia application.

1.1   Multicast Routing Realization

In the router software of our router, the multicast routing includes the following regulations:

●   IGMP runs between the router and the host in the LAN, which is used to track the group member relationship.

●   OLNK is a static multicast technology, which is used in the simple topology. It realizes the multicast forwarding and effectively saves CPU and bandwidth.

●   PIM-DM, PIM-SM and DVMRP is dynamic multicast routing protocols. They run between routeres and realizes the multicast forwarding by creating the multicast routing table.

The following figure shows the multicast protocols used in the IP multicast applications:
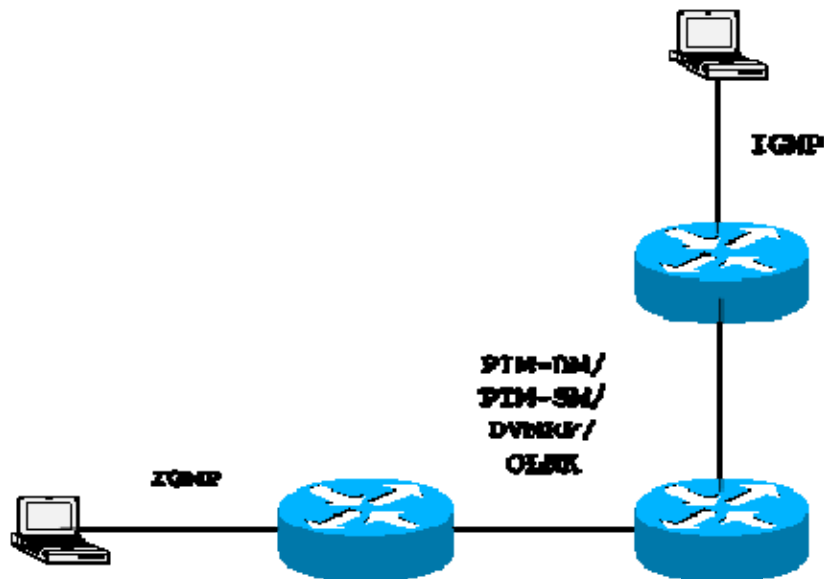
1.2　Multicast Routing Configuration Task List

1.2.1　Basic Multicast Configuration Task List

- Starting up the multicast routing (mandatory)
- Configuring TTL threshold (optional)
- Canceling rapid multicast forwarding (optional)
- Configuring static multicast route (optional)
- Configuring multicast boundary (optional)
- Configuring multicast helper (optional)
- Configuring Stub multicast route (optional)
- Monitoring and maintaining multicast route (optional)

1.2.2　IGMP Configuration Task List

- Modifying the current version of IGMP
- Configuring the IGMP query interval
- Configuring IGMP Querier interval
- Configuring the maximum response time of IGMP
- Configuring the query interval of the last IGMP group member
- Static IGMP configuration

- Configuring the IGMP **Immediate-leave** list

1.2.3   PIM-DM Configuration Task List

- Regulating the timer

- Designate the PIM-DM version

- Configuring the state refreshment

- Configuring the filtration list

- Setting the DR priority

- Clearing (S,G) information

1.2.4   PIM-SM Configuration Task List

- Configuring static RP

- Configuring standby BSR

- Configuring standby RP

- Displaying PIM-SM multicast routing

- Clearing multicast routes learned by PIM-SM

Chapter 2 **Basic Multicast Routing Configuration**

2.1 Starting up Multicast Routing

To allow the router software to forward the multicast message, you must start up the multicast routing. Run the following command in global configuration mode to start up the multicast message forwarding:

Command	Purpose
ip multicast-routing	Starts up the multicast routing.

2.2 Starting up the Multicast Function on the Port

When the multicast routing protocol runs on a port, the IGMP is activated on the port. The multicast routing protocols include OLNK, PIM-DM, PIM-SM and DVMRP. Only one multicast routing protocol is allowed to run on the same port. When the router connects multiple multicast domains, different multicast protocols can be run on different ports.

Although the router software can function as the multicast boundary router (MBR). If possible, do not simultaneously run multiple multicast routing protocols on the same router for some multicast routing protocols may be badly affected. For example, when PIM-DM and BIDIR PIM-SM simultaneously run, confusion is to occur.

2.2.1 Starting up PIM-DM

Run the following command to run PIM-DM on a port and then activate the multicast dense mode function:

Command	Purpose
ip pim-dm	Enters the port where PIM-DM is running and then activates PIM-DM multicast routing process in port configuration mode.

2.2.2 Starting up PIM-SM

To run PIM-DM on a port and activate the PIM-DM multicast, perform the following operation:

Command	Purpose
ip pim-sm	Enters a port where PIM-SM needs to run and then activates the PIM-SM multicast routing process in port configuration mode.

2.3　Configuring TTL Threshold

Run the command **ip multicast ttl-threshold** to configure the TTL threshold of the multicast message that is allowed to pass the port. Run the command **no ip multicast ttl-threshold** to use the default threshold value **1**.

Command	Purpose
ip multicast ttl-threshold *ttl-value*	Configures the TTL threshold on the port.

Example

The following example shows how the administrator configures the TTL threshold on a port:

interface ethernet 1/0

ip multicast ttl-threshold 200

2.4　Cancelling Rapid Multicast Forwarding

Run the command **ip multicast mroute-cache** to configure the rapid multicast forwarding function on a port. Run the command **no ip multicast mroute-cache** to cancel the rapid multicast forwarding function.

Command	Purpose
ip multicast mroute-cache	Enables the rapid multicast forwarding function on a port.

Example

The following example shows how the administrator cancels the rapid multicast forwarding function on a port:

interface ethernet 1/0
no ip mroute-cache

2.5　Configuring Static Multicast Route

The static multicast route allows that the multicast forwarding path is different from the unicast path. RPF check is performed when the multicast message is forwarded. The actual port receiving the message is the expected receiving port. That is, the port is the next-hop port of the unicast route that reaches the sender. If the unicast topology is same to the multicast topology, RPF check is reasonable. In some cases, the unicast path requires to be different from the multicast path.

Take the tunnel technology as an example. When a router in a path does not support the multicast protocol, the resolution is to configure the GRE tunnel between two routeres. In the following figure, each unicast router supports only the unicast message; each multicast router supports only the multicast message. The source host sends the multicast message to the destination host through MR1 and MR2. MR2 forwards the multicast message only when it is received through the tunnel. When the destination host sends the unicast message to the source host, the tunnel is also used. When the

tunnel technology is adopted, the message transmission speed is slower than that of the direct message transmission.
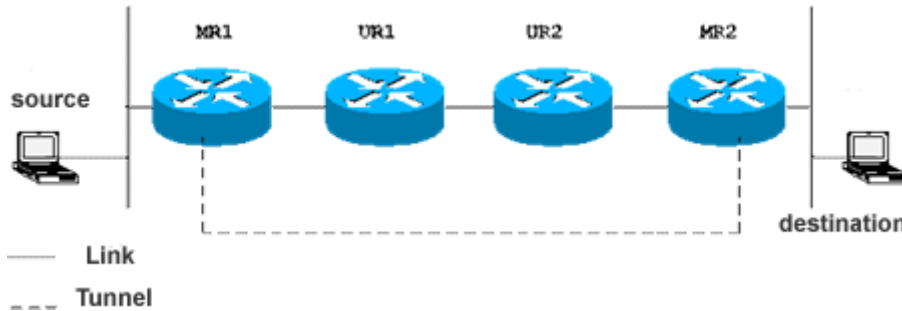
After the static multicast routing is configured, the router can perform the RPF check according to the configuration information. The RPF check is not based on the unicast routing table any more. Therefore, the multicast message goes through the tunnel, while the unicast message does not go through the tunnel. The static multicast route only exists in the local place. It will not be announced or forwarded.

Run the following command in global configuration mode to configure the static multicast route:

Command	Purpose
ip mroute *source-address mask rpf-address* **type** *number*[**distance**]	Configures the static multicast route.

2.6   Configuring IP Multicast Boundary

Run the command **ip multicast boundary** to configure the multicast boundary for the port. Run the command **no ip multicast boundary** to cancel the configured boundary. The commands used in the second configuration will replace the commands used in the first configuration.

Command	Purpose
ip multicast boundary *access-list*	Configures the multicast boundary for the port.

Example

The following example shows how to configure the management boundary for a port:

interface ethernet 0/0

ip multicast boundary acl

ip access-list standard acl

permit 192.168.20.97 255.255.255.0

2.7   Configuring IP Multicast Rate Control

Run the command **ip multicast rate-limit** to limit the rate of receiving and sending the multicast message in a source/group range. Run the command **no ip multicast rate-limit** to cancel the rate limitation.

Run the following command to limit the input rate of a multicast flow to n kbps.

Command	Purpose
ip multicast rate-limit in group-list *access-list*1 source-list *access-list*2 nkbps	Configures the maximum input rate limitation of the multicast flow in a certain range.

Run the following command to limit the output rate of a multicast flow to n kbps

Command	Purpose
ip multicast rate-limit out *group-list access-list*1 *source-list access-list*2 kbps	Configures the maximum output rate limitation of the multicast flow in a certain range.

2.8   Configuring IP Multicast Helper

Run the command **ip multicast helper-map** to use the multicast route to connect two broadcast networks in the multicast network. Run the command **no ip multicast helper-map** to cancel the command.

Command	Purpose
interface *type number*	Enters the interface configuration mode.
ip multicast helper-map broadcast *group-address access-list*	Configures the command **ip multicast helper** to convert the broadcast message to the multicast message.
ip directed-broadcast	Allows the directional broadcast.
ip forward-protocol [*port*]	Configures the port number allowing to forward the message.

On the last-hop router connecting the destination broadcast network, perform the following operations:

Command	Purpose
interface *type number*	Enters the interface configuration mode.
ip directed-broadcast	Allows the directional broadcast.
ip multicast helper-map *group-address broadcast-address access-list*	Configures the command **ip multicast helper** to convert the multicast message to the broadcast message.
ip forward-protocol [port]	Configures the port number allowing to forward the message.

Example

The following example shows how to configure the command **ip multicast helper**.

The configuration of the router is shown in the following figure. Configure the command **ip directed-broadcast** on the e0 port of the first-hop router to handle the directional message. Configure **ip multicast helper-map broadcast 230.0.0.1 testacl1**, allowing to convert the UDP broadcast message with port number 4000 that is sent from the source address 192.168.20.97/24 to the multicast message with the destination address 230.0.0.1.

Configure the command **ip directed-broadcast** on the e1 port of the last-hop router to handle the directional message. Configure **ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2**, allowing to convert the multicast message with port number 4000 and the destination address 230.0.0.1 that is sent from the source address 192.168.20.97/24 to the broadcast message with the destination address 172.10.255.255.

In the first-hop router connecting the source broadcast network, perform the following operations: (the router is configured on the VLAN port)

interface ethernet 0

ip directed-broadcast

ip multicast helper-map broadcast 230.0.0.1 testacl

ip pim-dm

!

ip access-list extended testacl   permit udp 192.168.20.97 255.255.255.0 any

ip forward-protocol udp 4000

In the last-hop router connecting the destination broadcast network, perform the following operations:

interface ethernet 1

ip directed-broadcast

ip multicast helper-map 230.0.0.1 172.10.255.255 testacl2

ip pim-dm

!

ip access-list extended testacl2   permit udp 192.168.20.97 255.255.255.0 any

ip forward-protocol udp 4000

2.9   Configuring Stub Multicast Route

Run the commands **ip igmp helper-address** and **ip pim-dm neighbor-filter** to configure the Stub multicast route.

On the port where the stub router and the host are connected, perform the following operations:

Command	Purpose
interface *type number*	Enters the interface configuration mode.
ip igmp helper-address *destination-address*	Configures the command **ip igmp helper-address** to forward the multicast message to the central router.

On the port where the central router and the stub router are connected, perform the following operations:

Command	Purpose
interface *type number*	Enters the interface configuration mode.
ip pim neighbor-filter *access-list*	Filters all **pim** messages on the stub router.

Example

The configuration of router A and B is shown as follows:

Stub Router A Configuration

ip multicast-routing

ip pim-dm

ip igmp helper-address 10.0.0.2

Central Router B Configuration

ip multicast-routing

ip pim-dm

ip pim-dm neighbor-filter stubfilter

ip access-list stubfilter

deny 10.0.0.1

2.10　Monitoring and Maintaining Multicast Route

a. Clearing the multicast cache and the routing table

If special caches or the routing table is invalid, you need to clear its content. Run the following commands in management mode:

Command	Purpose
clear ip igmp group [*type number*] [*group-address* | *<cr>*]	Clears the items in the IGMP cache.
clear ip mroute *[* | group-address | source-address]*	Clears the items in the multicast routing table.

b. Displaying the multicast routing table and system statistics information

The detailed information about the IP multicast routing table, cache or database helps to judge how the resources are used and to resolve network problems.

Run the following commands in management mode to display the statistics information about the multicast route:

Command	Purpose
show ip igmp groups [*type number* | *group-address*] [detail]	Displays the information about the multicast group in the IGMP cache.
show ip igmp interface [*type number*]	Displays the IGMP configuration information on the interface.
show ip mroute mfc	Displays the multicast forwarding cache.
show ip rpf [**ucast | mstatic | pim-dm** | **pim-sm** | **dvmrp**] *source-address*	Displays the RPF information.

Chapter 3 **IGMP Configuration**

3.1 Overview

a. IGMP

Internet Group Management Protocol (IGMP) is a protocol used to manage multicast group members. IGMP is an asymmetric protocol, containing the host side and the switch side. At the host side, the IGMP protocol regulates how the host, the multicast group member, reports the multicast group it belongs to and how the host responds to the query message from the switch. At the switch side, the IGMP protocol regulates how the IGMP-supported switch learns the multicast group member ID of the hosts in the local network and how to modify the stored multicast group member information according to the report message from the host.

Since our switches support the IGMP Router protocol, the multicast routing protocol can be provided with the information about the multicast group members in the current network and the switch decides whether to forward the multicast message. In a word, to enable the switch support the multicast process of the IP message, the switch need be configured to support the multicast routing protocol and the IGMP Router protocol. Currently, our switches support the IGMP Router protocol and version 3 IGMP, the latest version.

There is no independent startup commands for IGMP. The function of the IGMP-Router protocol is started up through the multicast routing protocol.

b. OLNK

Strictly speaking, the IGMP only-link protocol (OLNK) is not a multicast routing protocol because it has no interaction process as other protocols. However, in some special cases, running OLNK in the simple topology will get nice results. Similar to the PIM-DM protocol which also has no negotiation process, OLNK can handle the change of IGMP group members and promptly adjust the RPF interface according to the topology change. In this way, OLNK ensures the multicast forwarding and prevents the control messages of the multicast routing protocol from occupying the bandwidth.

3.2 IGMP Configuration

The commands to configure the attributes of the IGMP-Router mainly are the commands to adjust the IGMP parameters. The following is to describe these commands. For details about these commands, refer to explanation documents relative to the IGMP commands.

3.2.1 Changing Current IGMP Version

Up to now, the IGMP protocol has three formal versions. The corresponding RFCs are RFC1112, RFC2236 and RFC3376. IGMP V1 supports only the function to record the

multicast group members. IGMP V2 can query the designated multicast group member, generates the leave message when an IGMP host leaves a multicast group, and shortens the change delay of the group member. IGMP V3 has additional functions to update and maintain the multicast group member IDs which correspond to the source host addresses. The IGMP Router protocol of IGMP V3 is fully compatible with the host side of IGMP V1 and IGMP V2. our switch software supports the IGMP Router protocols of the three IGMP versions.

You can configure the IGMP-Router function at different interfaces (the multicast routing protocol configured on different interfaces can start up the IGMP-Router function) and different versions of IGMP can be run on different interfaces.

Note that a multicast switch can start up the IGMP-Router function on only one of the ports that connect the same network.

Run the following command in interface configuration mode to change the version of the IGMP-Router protocol on a port:

Command	Purpose
ip igmp version *version_number*	Changes the IGMP version running on the current port.

3.2.2 Configuring IGMP Query Interval

No matter what version number of the current IGMP-Router protocol is, the multicast switch can send the IGMP General Query message every a certain time on the port where the IGMP-Router function is started. The transmission address is 224.0.0.1. The purpose of the multicast switch is to get the report message from the IGMP host and therefore know which multicast group each IGMP host in the network belongs to. The interval to send the General Query message is called as IGMP Query Interval. If the parameter IGMP Query Interval is set to a big value, the switch cannot immediately receive the information about which multicast group the current IGMP host belongs to. If the parameter IGMP Query Interval is set to a small value, the flow of the IGMP message is to increase in the current network.

Run the following command in interface configuration mode to modify the IGMP query interval on a port:

Command	Purpose
ip igmp query-interval *time*	Modifies the IGMP query interval on the current interface (unit: second).

3.2.3 Configuring IGMP Querier Interval

As to version 2 and version 3 of the IGMP-Router protocol, if another switch that runs the IGMP-Router protocol exists in the same network, you need to choose a querier. Querier stands for a switch that can send the query message (In fact, it is a port of the switch where the IGMP-Router protocol is enabled). Normally, one network has only one querier, that is, only one switch sends the IGMP Query message. There is no querier choice for IGMP-Router V1 because the multicast routing protocol decides which switch to send the IGMP Query message in IGMP-Router V1.

IGMP-Router V2 and IGMP-Router V3 have the same querier choice mechanism, that is, the switch with the minimum IP address is the querier in the network. The switch that is not the querier needs to save a clock to record the existence of the querier. If

the clock times out, the non-querier switch turns to be the querier until it receives the IGMP Query message from the switch with a smaller IP address.

For IGMP-Router V2, you can configure other querier intervals using the following command:

Command	Purpose
ip igmp querier-timeout *time*	Configures the interval for other queriers (unit: second).

For IGMP-Router V1, the interval of other queriers is useless. For IGMP-Router V3, the interval cannot be configured because it is decided by the protocol itself.

3.2.4   Configuring Maximum IGMP Response Time

For IGMP-Router V2 and IGMP-Router V3, special data field in the transmitted IGMP General Query message regulates the maximum response time of the IGMP host. That is, the IGMP host has to send the response message before the regulated maximum response time expires, indicating that the General Query message is received. If the maximum response time is set to a big value, the change of multicast group members delays. If the maximum response time is set to a small value, the flow of the IGMP message will be increased in the current network.

Note:

The maximum IGMP response time must be shorter than the IGMP query interval. If the value of the maximum response time is bigger than the query interval, the system will automatically set the maximum response time to **query-interval – 1**.

For IGMP-Router V2 and IGMP-Router V3, run the following command in interface configuration mode to set the maximum IGMP response time:

Command	Purpose
ip igmp query-max-response-time *time*	Configures the maximum IGMP response time (unit: second).

For IGMP-Router V1, the maximum IGMP response time is decided by the protocol itself. Therefore, the previous command is useless to IGMP-Router V1.

3.2.5   Configuring IGMP Query Interval for the Last Group Member

For IGMP-Router V2 and IGMP-Router V3, When the Group Specific Query message for a specific multicast group is sent, the query interval of the last group member will be used as the maximum response time of the host. That is, the IGMP host has to send the response message before the maximum response time of the last group member expires, indicating that the Group Specific Query message is received. If the IGMP host finds that it need not respond to the query message, it will not respond to the message after the interval. In this case, the multicast switch is to update the saved multicast group member information. If the query interval of the last group member is set to a big value, the change of the multicast group member delays. If the query interval of the last group member is set to a small value, the flow of the IGMP message is to increase in the current network.

For IGMP-Router V2 and IGMP-Router V3, run the following command in interface configuration mode to configure the IGMP query interval of the last group member:

Command	Purpose
ip igmp last-member-query-interval *time*	Configures the IGMP query interval of the last group member (unit: ms).

The previous command is useless for IGMP-Router V1.

3.2.6 Static IGMP Configuration

Besides the functions regulated by the IGMP-Router protocol, BODCOM's switches support the static multicast group configuration on the port. For the IGMP host, its multicast group member relationship may vary. Suppose the IGMP host only belongs to the multicast group **group1**, it receives the multicast message from and sends the multicast message to the multicast group **group1**. After a period of time, it may belong to the multicast group **group2**, and receives the multicast message from and sends the multicast message to the multicast group **group2**. After another period of time, the IGMP host may not belong to any multicast group. Therefore, the multicast group assignment information varies.

Different the above "dynamic multicast group", if a port is configured to belong to a static multicast group, the multicast routing protocol then takes the port as one that always receives and sends the multicast message of the multicast group. To be better compatible with IGMP-Router V3, the static multicast group can be configured to receive the multicast message from the designated source address, that is, the source-filter function is added when the multicast message is received.

Run the following command in interface configuration mode to configure the static multicast group for a port:

Command	Purpose
ip igmp static-group { * | *group-address*} {**include** *source-address* | *<cr>* }	Configures the static multicast group attribute for a port.

3.2.7 Configuring the IGMP Immediate-leave List

If IGMP V2 is started up on a port of the switch and the network that the port connects has only one IGMP host, you can realize the Immediate Leave function of the IGMP host by configuring the **IGMP Immediate-leave** list. According to the regulations of IGMP V2, when a host leaves a specific multicast group, the host will send the Leave message to all multicast switches. After receiving the Leave message, the multicast switches send the Group Specific message to confirm whether any multicast message to be received from or sent to the multicast group by the host exists on the port. If the Immediate Leave function is configured, no message need be interacted between the IGMP host and the multicast switch, the change of the multicast group member IDs will not be delayed.

Note:

The command can be configured both in global configuration mode and in interface configuration mode. The priority of the command configured in global configuration mode is higher than that configured in interface configuration mode. If the command is first configured in global configuration mode, the command configured in interface configuration mode will be omitted. If the command is first configured in interface configuration mode, the command configured in global configuration mode will delete the command configured in interface configuration mode.

For IGMP-Router V2, run the following command in interface configuration mode to configure the IGMP **Immediate-leave** list:

Command	Purpose
ip igmp immediate-leave group-list *list-name*	Configures the access list that realizes the function to immediately leave the multicast group for the IGMP host.
ip access-list standard *list-name*	Creates a standard IP access list named **list-name**.
permit *source-address*	Configures the IP address for the IGMP host that will realize the immediate-leave function in standard access-list configuration mode.

The previous command is invalid to IGMP-Router V1 and IGMP-Router V3.

3.3   IGMP Characteristic Configuration Example

All configurations about the IGMP characteristics are performed in VLAN port.

a. Example for changing the IGMP version

The IGMP-Router protocol of latter version is compatible with the IGMP host of low version, but cannot be compatible with the IGMP-Router protocol of the earlier version. Therefore, if, there are switches running the IGMP-Router protocol of the earlier version in the current network, you need to change the IGMP-Router protocol of latter version to the IGMP-Router protocol of earliest version in the same network segment.

Suppose the administrator knows that switches running IGMP-Router V1 and IGMP-Router V2 exist in a network that the local switch connects, the administrator needs to change the version of the IGMP-Router protocol from version 2 to version 1 on a port of the switch that runs IGMP-Router V2.

interface ethernet 1/0
ip igmp version 1

b. IGMP query interval configuration example

The following example shows how to modify the IGMP query interval to 50 seconds on the interface **ethernet 1/0**:

interface ethernet 1/0
ip igmp query-interval 50

c. IGMP Querier interval configuration example

The following example shows how to modify the IGMP Querier interval to 100 seconds on the interface **ethernet 1/0**:

interface ethernet 1/0
ip igmp querier-timeout 100

d. Maximum IGMP response time example

The following example shows how to modify the maximum IGMP response time to 15 seconds on the interface **ethernet 1/0**:

interface ethernet 1/0

ip igmp query-max-response-time 15

e. Example for configuring IGMP query interval for the last group member

The following example shows how to modify the IGMP query interval of the last group member to 2000 ms on the interface ethernet 1/0:

interface ethernet 1/0

ip igmp last-member-query-interval 2000

f. Static IGMP configuration example

The configuration command of the static multicast group can define different classes of static multicast groups by adopting different parameters. The following examples shows the results of running different command parameter.

interface ethernet 1/0

ip igmp static-group *

The previous configuration command configures all static multicast groups on the interface ethernet 1/0. The multicast routing protocol is to forward all IP multicast messages to the interface ethernet 1/0.

interface ethernet 1/0

ip igmp static-group 224.1.1.7

The previous configuration command configures the static multicast group 224.1.1.7 on the interface ethernet 1/0, that is, the interface belongs to the multicast group 224.1.1.7. The multicast routing protocol is to forward all IP multicast messages that are finally sent to the multicast group 224.1.1.7 to the interface ethernet 1/0.

interface ethernet 1/0

ip igmp static-group 224.1.1.7 include 192.168.20.168

The previous configuration command configures the static multicast group 224.1.1.7 on the interface ethernet 0/0, and defines source-filter of the multicast group as 192.168.20.168. That is, the interface belongs to the multicast group 224.1.1.7, but it only receives the IP multicast messages from 192.168.20.168. The multicast routing protocol is to forward IP multicast messages that are received from 192.168.20.168 and finally sent to the multicast group 224.1.1.7 to the interface ethernet 0/0.

Run the following command in interface configuration mode to receive the IP multicast message that is from 192.168.20.169 and finally sent to the multicast group 224.1.1.7:

ip igmp static-group 224.1.1.7 include 192.168.20.169

The previous command can be executed for many times to define different source addresses.

Note:

In a multicast group, the multicast group information cannot be simultaneously configured both for a specific source address and for all source addresses. The command used in the later configuration will be omitted. For example, If you run the command **ip igmp static-group 224.1.1.7 include 192.168.20.168** after the command **ip igmp static-group 224.1.1.7** is executed, the command **ip igmp static-group 224.1.1.7 include 192.168.20.168** will be omitted.

g. IGMP Immediate-leave list configuration example

The following example shows how to set the access list to **imme-leave** on the interface ethernet 1/0 with the **immediate-leave** function and to add the IP address 192.168.20.168 of the IGMP host to the access list. The configuration ensures that the IGMP host with IP address 192.168.20.168 realizes the **immediate-leave** function.

interface ethernet 1/0

ip igmp immediate-leave imme-leave

exit

ip access-list standard imme-leave

permit 192.168.20.168

Chapter 4   **PIM-DM Configuration**

4.1   PIM-DM Introduction

Protocol Independent Multicast Dense Mode (PIM-DM) is a multicast routing protocol in dense mode. By default, when the multicast source starts to send the multicast data, all network nodes in the domain receive the data. Therefore, PIM-DM forwards the multicast packets in broadcast-pruning mode. When the multicast source starts to send data, the switches alongside forward the multicast packets to all PIM-activated interfaces except the RPF interface. In this way, all network nodes in the PIM-DM domain can receive these multicast packets. To finish the multicast forwarding, the switches alongside need create the corresponding multicast routing item (S,G) for group G and its source S. The routing item (S,G) includes the multicast source address, multicast group address, incoming interface, outgoing interface list, timer and logo.

If there is no multicast group member in a certain network segment, PIM-DM will send the pruning information, prune the forwarding interface connecting the network segment and then establish the pruning state. The pruning state corresponds to the timeout timer. When the timer times out, the pruning state turns to be the forwarding state again and the multicast data can be forwarded along these branches. Additionally, the pruning state contains information about the multicast source and the multicast group. When the multicast group member appears in the pruning area, PIM-DM actively sends the graft message to the upper field without waiting for the pruning state of the upper field to time out, turning the pruning state to the forwarding state.

As long as source S still sends information to group G, the first-hop switch will periodically send the refreshing information of the routing item (S,G) to the nether original broadcast tree to finish refreshing. The state refreshing mechanism of PIM-DM can refresh the state of the downstream, ensuring that the pruning of the broadcast tree does not time out.

In the multi-access network, besides the DR selection, PIM-DM also introduces the following mechanisms:

● Use the assertion mechanism to select the unique forwarder to prevent the multicast packet from being repeatedly forwarded.

● Use the add/prune restraint mechanism to reduce redundant add/prune information.

● Use the pruning deny mechanism to deny improper pruning actions.

In the PIM-DM domain, the switches that run PIM-DM periodically send the Hello information to achieve the following purposes:

● Discover neighboring PIM switches.

● Judge leaf networks and leaf switches.

● Select the designated router (DR) in the multi-access network.

To be compatible with IGMP v1, PIM-DM is in charge of the DR choice. When all PIM neighboring routers on the interface support DR Priority, the neighboring router with higher priority is selected as the DR. If the priority is the same, the neighboring router with the maximum interface IP value is selected as the DR. If the priority is not shown in the Hello message of multiple routers, the router whose interface has the biggest IP value is selected as the DR.

The PIM-DM v2 of DBCOM's switches supports the neighbor filtration list, CIDR, VLSM and IGMP v1-v3.

4.2   Configuring PIM-DM

4.2.1   Modifying Timer

The routing protocol adopts several timers to judge the transmission frequency of Hello message and state-refresh control message. The interval to transmit the Hello message affects whether the neighbor relationship can correctly created.

Run the following commands in switch configuration mode to regulate the timer:

Command	Purpose
ip pim-dm hello-interval	Sets the interval (unit: second) to send the Hello message from the interface and the neighbor.
ip pim-dm state-refresh origination-interval	For the first-hop switch directly connecting the source, the interval to send the state-refresh message is only valid to the configurations at the upstream ports. For the following switches, the interval is the period to receive and handle the state-refresh message.

4.2.2   Configuring State-Refresh

The state-refresh control information of the PIM-DM is forwarded in management mode by default. The configuration commands in interface configuration mode are effective only to the configurations at the upstream ports when the first-hop switch directly connecting the source sends the state-refresh message periodically. For the following switches, the interval is the period to receive and handle the state-refresh message.

Command	Purpose
no ip pim-dm state-refresh disable	Allows to send and receive the state-refresh message on the port.
ip pim-dm state-refresh origination-interval	Configures the interval to send and receive the state-refresh message on the port.

4.2.3   Configuring Filtration List

PIM-DM does not set the filtration list by default. The referred filtration list includes the neighbor filtration list and the multicast boundary filtration list. The filtration list requires to be configured in interface configuration mode.

To forbid a switch or switches at a network segment to join in the PIM-DM negotiation, the neighbor filtration list need be configured. To forbid or permit some groups to pass the local region, the multicast boundary filtration list need be configured.

Command	Purpose
ip pim-dm neighor-filter	Configures the neighbor filtration list.
ip multicast boundary	Configures the multicast boundary filtration list.

4.2.4   Setting DR Priority

To be compatible with IGMP v1, the DR choice is required. By default, the priority of the DR is set to **1**. When all PIM neighboring routers on the interface support DR Priority, the neighboring router with higher priority is selected as the DR. If the priority is the same, the neighboring router with the maximum interface IP value is selected as the DR. If the priority is not shown in the Hello message of multiple routers, the router whose interface has the biggest IP value is selected as the DR.

Run the following command in interface configuration mode:

Command	Purpose
ip pim-dm dr-priority	Configures the priority for the local DR on the designated port.

4.2.5   Clearing Item (S,G)

Normally, item (S,G) in the local MRT or the statistics value of the multicast message number forwarded through item (S,G) need be cleared. Run the following commands in management mode.

Command	Purpose
clear ip mroute pim-dm {*	*group* [*source*]}	Clears the item (S,G) in the local MRT. The operation is to delete all or part items of the local multicast routing table. Multicast message forwarding may be affected. The command is used to delete only the (S,G) items created by the PIM-DM multicast routing protocol on the upstream ports.
clear ip pim-dm interface	Resets the statistics value of multicast message forwarded by (S,G) on the PIM-DM port. The command is used to reset only the (S,G) items created by the PIM-DM multicast routing protocol on the upstream ports.

4.3 PIM-DM State-Refresh Configuration Example

Refer to section 4.2.2 "Configuring State-Refresh".

Chapter 5 **PIM-SM Configuration**

5.1 PIM-SM Introduction

Protocol Independent Multicast Spare Mode (PIM-SM) is a multicast routing protocol in sparse mode. In the PIM-SM domain, the switches that run PIM-SM periodically send the Hello information to achieve the following purposes:

● Discover neighboring PIM-SM switches.

● Select the designated router (DR) in the multi-access network.

As shown in the following figure, the DR sends the join/prune message to the directly-connected group members at the direction of multicast distribution tree, or sends the data of the directly-connected multicast source to the multicast distribution tree.
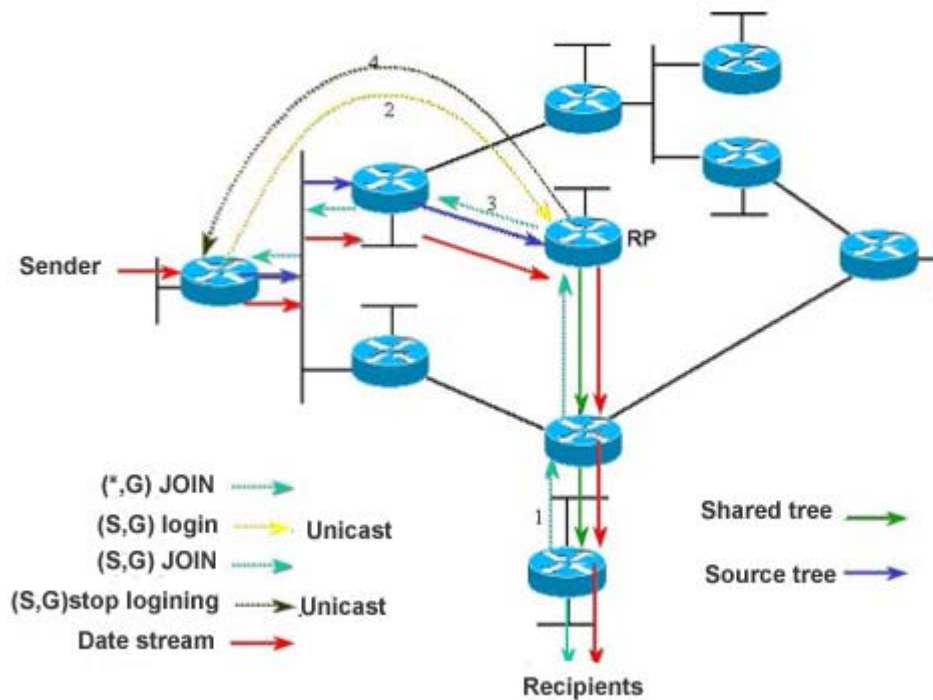
Figure 5-1   Join-in mechanism of PIM-SM

PIM-SM forwards the multicast packet by creating the multicast distribution tree. The multicast distribution tree can be classified into two groups: Shared Tree and Shortest Path Tree. Shared Tree takes the RP of group G as the root, while Shortest Path Tree takes the multicast source as the root. PIM-SM creates and maintains the multicast distribution tree through the displayed join/prune mode. As shown in Figure 5-1, when the DR receives a Join message from the receiving side, it will multicast a (*, G)-join message at each hop towards the RP of group G to join in the shared tree. When the

source host sends the multicast message to the group, the packet of the source host is packaged in the registration message and unicast to the RP by the DR; The RP then sends the unpackaged packet of the source host to each group member along the shared tree; The RP sends the (S,G)-join message to the first-hop switch towards the source's direction to join in the shortest path tree of the source; In this way, the packet of the source will be sent to the RP along the shortest path tree without being packaged; When the first multicast data arrives, the RP sends the registration-stop message to the DR of the source and the DR stops the registration-packaged process. Afterwards, the multicast data of the source is not packaged any more, but it will be sent to the RP along the shortest path three of the source and then sent to each group member by the RP along the shared tree. When the multicast data is not needed, the DR multicasts the Prune message hop by hop towards the RP of group G to prune the shared tree.

PIM-SM also deals with the RP choice mechanism. One or multiple candidate BSRs are configured in the PIM-SM domain. You can select a BSR among candidate BSRs according to certain regulations. Candidate RPs are also configured in the PIM-SM domain. These candidate RPs unicast the packets containing RP's address and multicast groups to the BSR. The BSR regularly generates the Bootstrap message containing a series of candidate RPs and corresponding group addresses. The Bootstrap message is sent hop by hop in the whole domain. The switch receives and stores the Bootstrap message. After the DR receives a report about a group member's relationship from the directly-connected host, if the DR has no the routing item of the group, the DR will map the group address to a candidate RP through the Hash algorithm. The DR then multicasts the Join/prune message hop by hop towards the RP. Finally, the DR packages the multicast data in the registration message and unicasts it to the RP.

5.2   Configuring PIM-SM

5.2.1   Starting up PIM-SM

Run the following command to run PIM-SM on the interface to activate the multicast function in sparse mode:

Command	Purpose
ip pim-sm	Enters the interface where PIM-SM needs to be run and activates the PIM-SM multicast routing process in interface configuration mode.

5.2.2   Configuring Static RP

If the network scale is small, you can configure the static RP to use PIM-SM. The RP configuration of all routers in the PIM-SM domain must be same, ensuring the PIM-SM multicast route is correct.

If some router in the PIM-SM domain runs the BSR, the RP check follows the order: the static RP with override configured is preferred. If the override is not configured for the static RP, the RP in the RP mapping list distributed by the BSR is preferred.

Run the following command in global configuration mode:

Command	Purpose
ip pim-sm rp-address rp-add [**override|acl-name**] **no ip pim-sm rp-address** rp-add	Configures the static RP for the local switch.

5.2.3 Configuring Candidate BSR

The configuration of the candidate RP can generate the unique global BSR in the PIM-SM domain. The global BSR collects and distributes the RP in the domain, ensuring the RP mapping is unique.

Run the following command in global configuration mode:

Command	Purpose
ip pim-sm bsr-candidate *type number* [*hash-mask-length*] [**priority**] **no ip pim-sm bsr-candidate** *type number*	Configures the local switch as the candidate BSR, and competes the global BSR by learning the BSM message.

5.2.4 Configuring Candidate RP

Configure the candidate RP to enable it to be sent to the BSR periodically and then be diffused to all PIM-SM routers in the domain, ensuring the RP mapping is unique.

Run the following command in global configuration mode:

Command	Purpose
ip pim-sm rp-candidate [**type** *number*] [**interval**|*group-list acl-name*] **no ip pim-sm rp-candidate** [**type** *number*]	Configures the local switch as the candidate RP. After the candidate RP is configured, it will be sent to the BSR periodically. The BSR then broadcasts all PIM-SM routers in the PIM-SM domain.

5.2.5 Displaying PIM-SM Multicast Route

Run the following command to check the multicast route information learned by PIM-SM:

Command	Purpose
show ip mroute pim-sm [*group-address*] [*source-address*] [**type** *number*] [**summary**] [**count**] [**active** *kbps*]	Displays the PIM-SM multicast route information.

5.2.6 Clearing Multicast Routes Learned by PIM-SM

Run the following command to clear multicast routes learned by PIM-SM:

Command	Purpose
clear ip mroute pim-sm [* | group-address] [source-address]	Clears information about the PIM-SM multicast routes.

5.3   Configuration Example

5.3.1   PIM-SM Configuration Example (The switch is configured on the VLAN port)

The following examples show how two switches learn and forward the PIM-SM multicast routes.

Device A:

```
!
ip multicast-routing
!
interface Loopback0
ip address 192.166.100.142 255.255.255.0
ip pim-sm
!
interface Ethernet1/1
ip address 192.166.1.142 255.255.255.0
ip pim-sm
ip pim-sm dr-priority 100
!
interface Serial2/0
ip address 192.168.21.142 255.255.255.0
physical-layer speed 128000
ip pim-sm
!
router rip
network 192.168.21.0
network 192.166.1.0
network 192.166.100.0
version 2
!
ip pim-sm bsr-candidate Loopback0 30 201
ip pim-sm rp-candidate Loopback0
!
```

Device B:

```
!
ip multicast-routing
!
interface Ethernet0/1
ip address 192.168.200.144 255.255.255.0
ip pim-sm
ip pim-sm dr-priority 200
!
interface Serial0/0
```

```
ip address 192.168.21.144 255.255.255.0
ip pim-sm
!
```

5.3.2   BSR Configuration Example (The switch is configured on the VLAN port)

The following example shows the BSR configuration of two switches.

Device A:

```
!
ip multicast-routing
!
interface Loopback0
ip address 192.166.100.142 255.255.255.0
ip pim-sm
!
interface Ethernet1/1
ip address 192.166.1.142 255.255.255.0
ip pim-sm
!
interface Serial2/0
ip address 192.168.21.142 255.255.255.0
physical-layer speed 128000
ip pim-sm
!
router rip
network 192.168.21.0
network 192.166.100.0
!
ip pim-sm bsr-candidate Loopback0 30 201
!
```

Device B:

```
!
ip multicast-routing
!
interface Loopback0
ip address 192.168.100.144 255.255.255.0
ip pim-sm
!
interface Ethernet0/1
ip address 192.168.200.144 255.255.255.0
ip pim-sm
!
interface Serial0/0
ip address 192.168.21.144 255.255.255.0
ip pim-sm
```

```
!
ip pim-sm bsr-candidate Loopback0 30
!
```

Chapter 6 **DVMRP Configuration**

6.1 DVMRP Overview

Distance Vector Multicast Routing Protocol (DVMRP) is the first protocol to support the selection of multi-goal broadcast paths. DVMRP is widely used on the MBone network, which is described carefully in RFC 1075. BVMRP of OUR routers is developed specially for the DVMRPv3 draft (draft-ietf-idmr-dvmrp-v3-101.txt), which is compatible with DVMRPv1 (RFC 1075).

DVMRP can construct different multicast distribution trees for different multicast routes. Each multicast distribution tree is the minimum spanning tree, which consists of the distribution source on the root and all reception/transmission hosts on the leaves. According to the hops of a packet on a path, the multicast distribution tree provides the shortest path from the distribution source to each reception host. When the multicast source begins to transmit information to the multicast group, the technology of graft and prune is used to construct the distribution tree.

DVMRP v3 of our routers supports the leaf node, the multicast source's mask, the unicast filtration list, the automatic summary and the manual summary.

6.2 DVMRP Configuration

6.2.1 Enabling DVMRP

To activate the multicast of the dense mode by running DVMRP, run the following commands:

Command	Purpose
ip dvmrp **mo ip dvmrp**	Enter the port on which DVMRP is run and activate the DVMRP multicast routing process in port configuration mode.

6.2.2 Configuring Route Summary

The cost of summary routes depends on the maximum cost of all subnet routes, which is used to speed up route calculation due to the forming of route loop.

When two or more ports of a router form route loops with other routers, it is recommended that the same summary mechanism is configured on these ports.

Run the following commands in port configuration mode:

Command	Purpose
[**no**]**ip dvmrp auto-summary**	Configure the automatic summary on the local router.

| [**no**]ip summary-address *network-address network-mask* | Configure the manual summary on the local router. |

6.2.3 Configuring the Mandatory Leaf Node

The mandatory leaf node forms the corresponding environment by omitting other routers on these ports.

Run the following command:

Command	Purpose
[**no**] **ip dvmrp force-leaf**	Set a port to be a leaf node.

6.2.4 Configuring the Route Filter

If a route filter is configured on a port, the received and transmitted routes can be filtered on this port.

Run the following command:

Command	Purpose
[**no**] **ip dvmrp route-filter** {**in|out**} *acl-name*	Configure a filter on a port to filtrate unnecessary routes.

6.2.5 Displaying the DVMRP Unicast Route

To browse unicast routing information that is learned by DVMRP, run the following command:

Command	Purpose
show ip dvmrp route [*network-address* [*network-mask*]]	Display the DVMRP unicast route.

6.2.6 Displaying the DVMRP multicast route

To browse multicast routing information that is learned by DVMRP, run the following command:

Command	Purpose
show ip mroute dvmrp [*source-address* [*group-address*]]	Display the DVMRP multicast route.

6.2.7 Deleting the DVMRP-learned multicast route

To delete multicast routing information that is learned by DVMRP, run the following command:

Command	Purpose
clear ip mroute dvmrp { * | *source-address* [*group-address*] }	Deletes the DVMRP multicast routes.

6.3 DVMRP Configuration Example

An example about the interconnection between Router A and Router B is given here. Because DVMRP of Cisco router is in passive mode, it is enough for Cisco router to start PIM-DM or PIM-SM.

Configuration of router A:

```
!
ip multicast-routing
!
interface Ethernet1/1
ip address 200.1.1.142 255.255.255.0
ip dvmrp
!
interface Ethernet2/1
ip address 192.168.20.142 255.255.255.0
ip dvmrp
!
```

Configuration of router B:

```
!
ip multicast-routing
!
interface FastEthernet0/0
ip address 192.168.20.204 255.255.255.0
ip pim dense-mode
!
interface FastEthernet0/1
ip address 100.1.20.204 255.255.255.0
ip pim dense-mode
!
```