Оглавление

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:
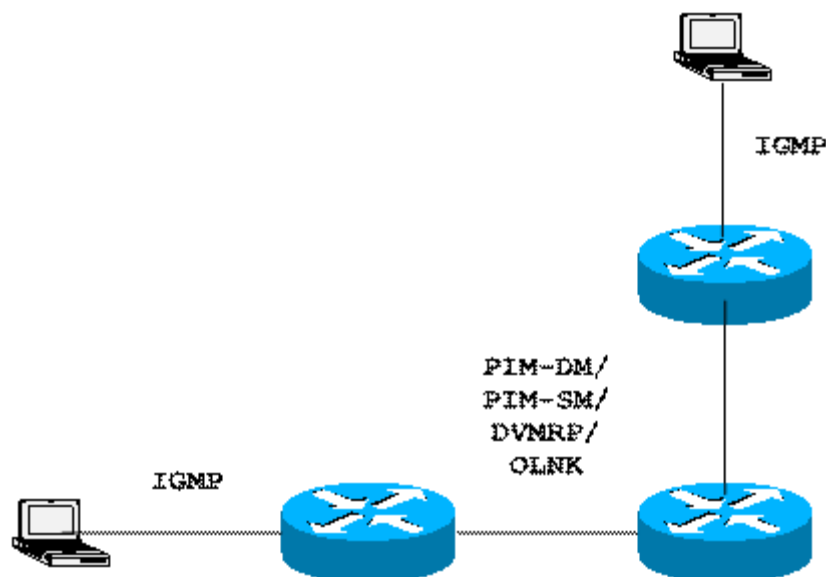
1.2. Multicast Routing Configuration Task List

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

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. 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
```

QTECH
МИР ДОСТУПНЕЕ

www.qtech.ru

```
ip access-list standard acl

permit 192.168.20.97 255.255.255.0
```

2.5. 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
```

2.6. 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
```

2.7. Monitoring and Maintaining Multicast Route

2.7.1. 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.

2.7.2. 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.

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, MY COMPANY' 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.

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

www.qtech.ru

compatible with the host side of IGMP V1 and IGMP V2. MY COMPANY's 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).

QTECH
МИР ДОСТУПНЕЕ   www.qtech.ru

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.

3.3.1. 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
```

3.3.2. 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
```

3.3.3. 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
```

3.3.4. 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
```

3.3.5. 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
```

3.3.6. 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.

3.3.7. 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
```

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. Designating the Version Number

PIM-DM of the router only supports PIM v2.

QTECH
МИР ДОСТУПНЕЕ

www.qtech.ru

As PIM v1 is out of date, we supports PIM v2 by default. The command here only aims to be compatible with the former in style.

Command	Purpose
ip pim-dm version *version*	Configures PIM-DM version on the switch logical port.

4.2.3. 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.

4.2.4. 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.

www.qtech.ru

| ip multicast boundary | Configures the multicast boundary filtration list. |

4.2.5. 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.

4.2.6. 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".

5. CONFIGURING PIM-SM

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.

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.

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. Enabling Global Multicast

Command:

ip multicast-routing

no ip multicast-routing

If you want to use the protocol pim-sm, run the command in the configuration mode:

switch_config#ip multicast-routing

Show running as follows:

!

ip multicast-routing

!

If you don't want to use the protocol pim-sm, run the command in the configuration mode:

switch_config #no ip multicast-routing

5.2.2. 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.

5.2.3. Configuring Neighbor Filter List

pim-sm needs to maintain neighbor relation in work. pim-sm finishes negotiation of the detection and related parameters through Hello information. Pim-sm forwards pim-sm hello packet by multicast periodically to all pim routers (224.0.0.13) and set up the neighbor relation by receiving hello information and agreed parameters. If one router receives Hello information before forwarding Hello information, the router will deem existence of the neighbor, otherwise, it will deem no existence of the neighbor.

Configure the neighbor filter list on the corresponding interface and check and filter the neighbor for the hello packet. If the neighbor filter list is deleted or the forbidden neighbor is relived just now, the neighbor information can only be acquired when the next hello period is appeared.

Steps for configuring neighbor access list:

1. Configure main ip address on the interface;
2. Port protocol up
3. Configure pim-sm on the interface;
4. Configure pim-sm standard access list on the interface and filter the neighbor.

Configuration instances:

switch_config#interface v9

switch_config_v9#ip address 172.20.21.172 255.255.255.0

switch_config_v9#ip pim-sm

switch_config_v9#ip pim-sm nbr-filter nbr_permit

switch_config_v9#exit

switch_config#ip access-list standard nbr_permit

switch_config_std_nacl#permit 172.20.21.174 255.255.255.0

Configuration result: enable hello packets from segment 172.20.21.0/24 and set up neighbor relation.

R172_config_std_nacl#show ip pim-s nei

PIM-SMv2 Neighbor Table

Neighbor	Interface	Uptime/Expires	DR
Address			Prior
172.20.21.173	v9	00:15:24/00:01:30	1(DR)

Change the configuration as follows and the interface v9 only enables hello packets from 172.20.21.174.

QTECH
МИР ДОСТУПНЕЕ   www.qtech.ru

S172_config_std_nacl#permit 172.20.21.174 255.255.255.255

The debug information is as follows:

2004-1-1 00:16:26 PIM-SM: rcvd hello from 172.20.21.173, filter by acl

The former established neighbor will be aged gradually until timeout:

S172#show ip pim-s nei

PIM-SMv2 Neighbor Table

Neighbor	Interface	Uptime/Expires	DR
Address			Prior
172.20.21.173	v9	00:17:21/00:00:03	1(DR)

5.2.4. DR Election

DR election is to select DR for the router segment by comparing the priority and IP address in the Hello packets of each router.

The role of DR plays:

1. For response on the host IGMP(v1) information, if the host connects two or more PIM-SM routers directly by the Ethernet, only DR informs these information and forwards packets (*,g) join. If DR and assert winner on the receiver end confronts, the former prevails.
2. DR on the multicast source generates original registration packets and register to RP.

If a new neighbor is found, DR is responsible for forwarding the local memorized BSM packets.

If the locak tries to become DR, enhance the local DR priority and IP address value in condition of the same DR priority.

Steps for configuring DR priority:

1. Configures main ip address on the interface;
2. Port protocol up;
3. Configure pim-sm on the interface;
4. Configure ip pim-sm dr-pri ** on the interface;

5.2.5. 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.

5.2.6. 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.

5.2.7. Configuring SPT-threshhold

When the data is forwarded on the switch, it needs to judge whether shift RPT to SPT. The evidence for this judge is spt-threshold. By default SPT switches if the receiver receives the first data packet. We can set the threshold of RPT switching to SPT; unit: KB/s. In general if RPT switches to SPT, there is no return.

switch_config#router pim-sm

switch_config_ps#spt-threshold 1000

5.2.8. Configuring SSM

SSM model needs support of IGMPv3 and enables IGMPv3 on the PIM-SM device of the receiver. SSM model can be realized by the subset function of pim-sm and the system enables functions of PIM-SM and SSM. When deploying pim-sm, it is recommend to enable pim-sm on all non-boundary interfaces.

QTECH
МИР ДОСТУПНЕЕ | www.qtech.ru

During the process of transmitting the information of multicast source to the receiver, whether pim-ssm or pim-sm is determined by whether the multicast group of the receiver prescribed channel (S, G) exists within the multicast group of pim-ssm. Interfaces which enables pim-sm will deem the multicast group within the range adopting the model "pim-ssm".

Before configuring the basic functions of pim-ssm, the unicast route needs to be configured first, which ensures the interaction of the inner network layer and available route.

Steps for configuring pim-ssm:

1. Enable pim-sm on the interface;
2. Enter pim-sm configuration mode and address range of SSM group address;
3. Configure other functions of pim-sm (optional).

Configuration instances:

switch_config#interface v8

switch_config_v8#ip addr 1.1.1.1 255.255.255.0

switch_config_v8#ip pim-sm

switch_config_v8#exit

switch_config#router pim-sm

switch_config_ps#ssm rang grp_range

switch_config_ps#exit

switch_config#ip access-list standard grp-range

switch_config_std_nacl#permit 233.1.0.0 255.255.0.0

switch_config_std_nacl#

The following configuration does not take the default 232.0.0.0/8 as the group range of SSM, but 233.1.0.0/8. If SSM is canceled, disable ssm related configuration with "no" in the configuration mode of pim-sm.

5.2.9. Configuring Management Domain sz

In the mechanism of non-management domain, one pim-sm domain only has an exclusive BSR. The whole network is controlled by the BSR. For better management, the whole pim-sm domain can be divided into many management domains: each management domain maintains one BSR respectively and serves the multicast group within a certain range; global domain also maintains one BSR, which serves all left multicast groups.

In the mechanism of management domain, the boundary of each management domain is consisted of ZBR and each management domain maintains one BSR, which serves the multicast group of a certain range. The packets(such as assert message and BSR BootStrap message) of multicast protocol belonging to this range cannot pass the boundary of the management domain.

In the network which applies the management domain mechanism, select BSR for different multicast groups from C-BSR. C-RP within the network only forward inform packets to the corresponding BSR and BSR summarizes these packets on RP-SET and inform all devices within the service management domain.

For a group, if you want to find its rp, find sz corresponding to this group based on the longest prefix and sub-mask prevails; and find the corresponding RP-SET in sz according to the prefix and sub-mask of the group, and then calculate rp.

Steps for configuring management domain:

1. On management boundary device ZBR, configuring the range of local management domain group.
2. In the management domain, enter the configuration of pim-sm:

Configure the group range of standby BSR and keep consistent with the management domain boundary.

Configure standby BSR and designate standby BSR port.

Configuration instances:

1. Configure the management domain range on ZBR
2. Sa_config_v9#ip pim-sm admin-scope 225.1.1.0 255.255.255.0
3. Configure the group range and port of standby BSR on domain pim-sm device

Sb_config#interface loopback1

Sb_config_l1#ip addr 1.1.1.1 255.255.255.0

Sb_config_l1#ip pim-sm

Sb_config#router pim-sm

Sb_config_ps#c-bsr admin-scope 225.1.1.0 255.255.255.0 30 200

Sb_config_ps#c-bsr loopback1 32 250

30,32 means the sub-mask length of hash, and 200, 250 means standby BSR priority. When there is inconsistency, the designated value when configuring standby BSR is superior to that of configuring management domain.

QTECH
МИР ДОСТУПНЕЕ   www.qtech.ru

5.2.10. Configuring Source Address of Registered Packets

By default, when DR on the data source forwarding register packets, the address with DR will be taken as the source address of the registered packets. We can designate any active pim-sm interface on the DR device as the source address of the registered packets.

Configuration instances:

Sb_config#interface loopback1

Sb_config_l1#ip addr 1.1.1.1 255.255.255.0

Sb_config_l1#ip pim-sm

Sb_config#router pim-sm

Sb_config_ps# reg-src loopback 1

Designate the main address of loopback1 as the source address of the registered packets.

5.2.11. Configuring anycast-rp

An individual RP has a great load in the domain of pim-sm. To lower such burden, we can designate many same rp. The multicast source and the receiver will forward registered packets and join requests based on the latest rp.

If there is no MSDP module introduced, the neighbor of anycast-rp must be clearly specified when configuring anycast-rp and the neighbor address and the port address acting as rp cannot be the same.

Refer to *Pim-sm Command Manual* for configuration instances.

5.2.12. 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.

5.2.13. 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
```

!