Content

Chapter 1 IPv4 Multicast Protocol

1.1 IPv4 Multicast Protocol Overview

This chapter will give an introduction to the configuration of IPv4 Multicast Protocol.

1.1.1 Introduction to Multicast

Various transmission modes can be adopted when the destination of packet (including data, sound and video) transmission is the minority users in the network. One way is to use Unicast mode, i.e. to set up a separate data transmission path for each user; or, to use Broadcast mode, which is to send messages to all users in the network, and they will receive the Broadcast messages no matter they need or not. For example, if there are 200 users in a network who want to receive the same packet, then the traditional solution is to send this packet for 200 times separately via Unicast to guarantee the users who need the data can get all data wanted, or send the data in the entire domain via Broadcast. Transferring the data in the whole range of network .The users who need these data can get directly from the network. Both modes waste a great deal of valuable bandwidth resource, and furthermore, Broadcast mode goes against the security and secrecy.

The emergence of IP Multicast technology solved this problem in time. The Multicast source only sends out the message once, Multicast Routing Protocol sets up tree-routing for Multicast data packet, and then the transferred packet just starts to be duplicated and distributed in the bifurcate crossing as far as possible. Thus the packet can be sent to every user who needs it accurately and effectively.

It should be noticed that it is not necessary for Multicast source to join in Multicast group. It sends data to some Multicast groups, but it is not necessarily a receiver of the group itself. There can be more than one source sending packets to a Multicast group simultaneously. There may exist routers in the network which do not support Multicast, but a Multicast router can encapsulate the Multicast packets into Unicast IP packets with tunnel mode to send them to the Multicast router next to it, which will take off the Unicast IP header and continue the Multicast transmission process, thus a big alteration of network structure is avoided. The primary advantages of Multicast are:

1. Enhance efficiency: reduce network traffic, lighten the load of server and CPU

2. Optimize performance: reduce redundant traffic
3. Distributed application: Enable Multipoint Application

1.1.2 Multicast Address

The destination address of Multicast message uses class D IP address with range from 224.0.0.0 to 239.255.255.255. D class address can not appear in the source IP address field of an IP message. In the process of Unicast data transmission, the transmission path of a data packet is from source address routing to destination address, and the transmission is performed with hop-by-hop principle. However, in IP Multicast environment, the destination addresses is a group instead of a single one, they form a group address. All message receivers will join in a group, and once they do, the data flowing to the group address will be sent to the receivers immediately and all members in the group will receive the data packets. The members in a Multicast group are dynamic, the hosts can join and leave the Multicast group at any time.

Multicast group can be permanent or temporary. Some of the Multicast group addresses are assigned officially; they are called Permanent Multicast Group. Permanent Multicast Group keeps its IP address fixed but its member structure can vary within. The member amount of Permanent Multicast Group can be arbitrary, even zero. The IP Multicast addresses which are not kept for use by Permanent Multicast Group can be utilized by temporary Multicast groups.

224.0.0.0 ～ 224.0.0.255 are reserved Multicast addresses (Permanent Group Address), address 224.0.0.0 is reserved but not assigned, and other addresses are used by Routing Protocol; 224.0.1.0～238.255.255.255 are Multicast addresses available to users（Temporary Group Address） and are valid in the entire domain of the network; 239.0.0.0～239.255.255.255 are local management Multicast addresses, which are valid only in specific local domain. Frequently used reserved multicast address list is as follows:

Benchmark address (reserved)

224.0.0.1 Address of all hosts

224.0.0.2 Address of all Multicast Routers

224.0.0.3 Unassigned

224.0.0.4 DVMRP Router

224.0.0.5 OSPF Router

224.0.0.6 OSPF DR

224.0.0.7 ST Router

224.0.0.8 ST host

224.0.0.9 RIP-2 Router

224.0.0.10 IGRP Router

224.0.0.11 Active Agent

224.0.0.12 DHCP Server/Relay Agent

224.0.0.13 All PIM Routers

224.0.0.14 RSVP Encapsulation

224.0.0.15 All CBT Routers

224.0.0.16 Specified SBM

224.0.0.17 All SBMS

224.0.0.18 VRRP

224.0.0.22 IGMP

When Ethernet transmits Unicast IP messages, the destination MAC address it uses is the receiver's MAC address. But in transmitting Multicast packets, the transmission destination is not a specific receiver any more, but a group with uncertain members, thus Multicast MAC address is used. Multicast MAC address is corresponding to Multicast IP address. It is prescribed in IANA (Internet Assigned Number Authority) that the higher 25 bits in Multicast MAC address is 0x01005e, and the lower 23bits in MAC address is the lower 23bits in Multicast IP address.

Since only 23bits out of the lower 28bits in IP Multicast address are mapped into MAC address, therefore there are 32 IP Multicast addresses which are mapped into the same MAC address.

1.1.3 IP Multicast Packet Transmission

In Multicast mode, the source host sends packets to the host group indicated by the Multicast group address in the destination address field of IP data packet. Unlike Unicast mode, Multicast data packet must be forwarded to a number of external interfaces to be sent to all receiver sites in Multicast mode, thus Multicast transmission procedure is more complicated than Unicast transmission procedure.

In order to guarantee that all Multicast packets get to the router via the shortest path, the receipt interface of the Multicast packet must be checked in some certain way based on Unicast router table; this checking mechanism is the basis for most Multicast Routing Protocol to forward in Multicast mode --- RPF (Reverse Path Forwarding) check. Multicast router makes use of the impressed packet source address to query Unicast Router Table or independent Multicast Router Table to determine if the packet ingress interface is on the shortest path from receipt site to source address. If shortest path Tree is used, then the source address is the address of source host which sends Multicast Data Packets; if Shared Tree is used, then the source address is the address of the root of the Shared-Tree. When Multicast data packet gets to the router, if RPF check passes, then the data packet is forwarded according to Multicast forward item, and the data packet will be discarded else wise.

1.1.4 IP Multicast Application

IP Multicast technology has effectively solved the problem of sending in single point and receiving in multipoint. It has achieved the effective data transmission from a point to multiple points, saved a great deal of network bandwidth and reduced network load. Making use of the Multicast property of network, some new value-added operations can be supplied conveniently. In Information Service areas such as online living broadcast, network TV, remote education, remote medicine, real time video/audio meeting, the following applications may be supplied:

1) Application of Multimedia and Streaming Media
2) Data repository, finance application (stock) etc
3) Any data distribution application of “one point to multiple points”

In the situation of more and more multimedia operations in IP network, Multicast has tremendous market potential and Multicast operation will be generalized and popularized.

1.2 PIM-DM

1.2.1 Introduction to PIM-DM

PIM-DM（Protocol Independent Multicast, Dense Mode）is a Multicast Routing Protocol in dense mode which applies to small network. The members of multicast group are relatively dense under this kind of network environment.

The working process of PIM-DM can be summarized as: Neighbor Discovery, Flooding & Prune, and Graft.

1. Neigh hour Discovery

After PIM-DM router is enabled, Hello message is required to discover neighbors. The network nodes which run PIM-DM use Hello message to contact each other. PIM-DM Hello message is sent periodically.

2. Flooding & Prune of process

PIM-DM assumes all hosts on the network are ready to receive Multicast data. When some Multicast Source begins to send data to a Multicast Group G, after receiving the Multicast packet, the router will make RPF check first according to the Unicast table. If the check passes, the router will create a (S, G) table entry and transmit the Multicast packet to all downstream PIM-DM nodes on the network (Flooding). If the RPF check fails, i.e. the Multicast packet is input from the incorrect interface, and then the message is discarded. After this procedure, in the PIM-DM Multicast domain, every node will create a (S, G) table entry. If there is no Multicast group member in the downstream nodes, then a Prune

message is sent to upstream nodes to notify them not to transmit data of this Multicast group any more. After receiving Prune message, the upstream nodes will delete the corresponding interface from the output interface list to which their Multicast transmission table entry (S, G) corresponds. Thus a SPT（Shortest Path Tree, SPT） tree with source S as root is created. The Prune process is initiated by leaf router first.

The process above is called Flooding & Prune process. Each pruned node also provides time-out mechanics at the same time. When Prune is timed-out, the router will restart Flooding & Prune process. The PIM-DM Flooding & Prune is periodically processed.

3. RPF Check

With RPF Check, PIM-DM makes use of existing Unicast routing table to establish a Multicast transmission tree initiating from data source. When a Multicast packet arrives, the router will determine whether the coming path is correct first. If the arrival interface is the interface connected to Multicast source indicated by Unicast routing, then this Multicast packet is considered to be from the correct path. Otherwise the Multicast packet is to be discarded as redundant message. The Unicast routing message used as path judgment can root in any Unicast Routing Protocol, such as messages found by RIP, OSPF, etc. It doesn't rely on any specific Unicast Routing Protocol.

4. Assert Mechanism

If each of two Multicast routers A and B on the same LAN segment has a receiving route respectively and both will transmit the Multicast packet to the LAN after receiving the Multicast data packet sent by the Multicast Source S, then the downstream node Multicast router C will receive two exactly same Multicast packets. The router needs to choose a unique transmitter through Assert mechanism after it detects this situation. An optimal transmission path is selected through sending out Assert packet. If the priority and cost of two or more path are same, then the node with larger IP address is taken as the upstream neighbor of the (S, G) entry and in charge of the transmission of the (S, G) Multicast packet.

5. Graft

When the pruned downstream node needs to recover to transmission status, this node uses Graft Packet to notify upstream nodes to restore multicast data transmission.

1.2.2 PIM-DM Configuration Task List

1. Enable PIM-DM (Required)
2. Configure static multicast routing entries(Optional)
3. Configure additional PIM-DM parameters(Optional)
   a) Configure the interval for PIM-DM hello messages
   b) Configure the interval for state-refresh messages

c) Configure the boundary interfaces

d) Configure the management boundary

4. Disable PIM-DM protocol

1. Enable the PIM-DM protocol

When configuring the PIM-DM protocol on Layer 3 switches, PIM multicasting should be enabled globally, then PIM-DM can be enabled for specific interfaces.

Command	Explanation
Global Mode	
ip pim multicast-routing **no ip pim multicast-routing**	To enable PIM-DM globally for all the interfaces (However, in order to make PIM-DM work for specific interfaces, the following command should be issued).

And then turn on PIM-SM switch on the interface

Command	Explanation
Interface Configuration Mode	
ip pim dense-mode	To enable PIM-DM protocol for the specified interface.(Required)

2. Configure static multicast routing entries

Command	Explanation
Global Configuration Mode	
ip mroute *<A.B.C.D>* *<A.B.C.D>* *<ifname>* *<.ifname>* **no ip mroute *<A.B.C.D>* *<A.B.C.D>* [*<ifname>* *<.ifname>*]**	To configure a static multicast routing entry. The no form of this command will remove the specified entry.

3. Configure additional PIM-DM parameters

a) Configure the interval for PIM-DM hello messages

Command	Explanation
Interface Configuration Mode	
ip pim hello-interval < *interval*> **no ip pim hello-interval**	To configure the interval for PIM-DM hello messages. The no form of this command will restore the interval to the default value.

b) Configure the interval for state-refresh messages

Command	Explanation
Interface Configuration Mode	

ip pim state-refresh origination-interval **no ip pim state-refresh origination-interval**	To configure the interval for sending PIM-DM state-refresh packets. The no form of this command will restore the default value.

c) Configure the boundary interfaces

Command	Explanation
Interface Configuration Mode	
ip pim bsr-border **no ip pim bsr-border**	To configure the interface as the boundary of PIM-DM protocol. On the boundary interface, BSR messages will not be sent or received. The network connected the interface is considered as directly connected network. The no form of this command will remove the configuration.

d) Configure the management boundary

Command	Explanation
Interface Configuration Mode	
ip pim scope-border <*1-99* >|<*acl_name*> **no ip pim scope-border**	To configure PIM-DM management boundary for the interface and apply ACL for the management boundary. With default settings, 239.0.0.0/8 is considered as the scope of the management group. If ACL is configured, then the scope specified by ACL permit command is the scope of the management group. The no form of this command will remove the configuration.

4. Disable PIM-DM protocol

Command	Explanation
Interface Configuration Mode	
no ip pim dense-mode	To disable the PIM-DM protocol for the interface.
Global Configuration Mode	
no ip pim multicast-routing	To disable PIM-DM globally.

1.2.3 PIM-DM Configuration Examples

As shown in the following figure, add the Ethernet interfaces of Switch A and Switch B

to corresponding vlan, and enable PIM-DM Protocol on each vlan interface.

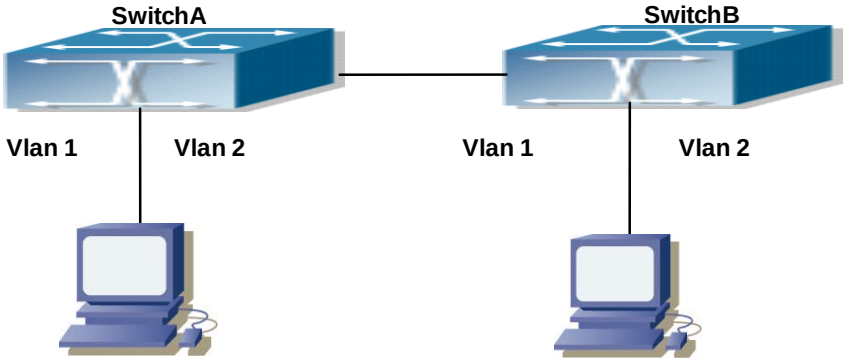


Fig 1-1 PIM-DM Typical Environment

The configuration procedure for SwitchA and SwitchB is as follows:

(1) Configure SwitchA:

Switch(config)#ip pim multicast-routing

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)# ip address 10.1.1.1 255.255.255.0

Switch(Config-if-Vlan1)# ip pim dense-mode

Switch(Config-if-Vlan1)#exit

Switch(config)#interface vlan2

Switch(Config-if-Vlan2)# ip address 12.1.1.1 255.255.255.0

Switch(Config-if-Vlan2)# ip pim dense-mode

(2) Configure SwitchB:

Switch(config)#ip pim multicast-routing

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)# ip address 12.1.1.2 255.255.255.0

Switch(Config-if-Vlan1)# ip pim dense-mode

Switch(Config-if-Vlan1)#exit

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)# ip address 20.1.1.1 255.255.255.0

Switch(Config-if-Vlan2)# ip pim dense-mode

At the same time, you should pay attention to the configuration of Unicast Routing Protocol, assure that each device can communicate with each other in the network layer, and be able to implement dynamic routing update in virtue of Unicast Routing Protocol.

1.2.4 PIM-DM Troubleshooting

In configuring and using PIM-DM Protocol, PIM-DM Protocol might not operate normally caused by physical connection or incorrect configuration. Therefore, the user

should pay attention to the following issues:

- ☞ To assure that physical connection is correct
- ☞ To assure the Protocol of Interface and Link is UP (use show interface command)
- ☞ To assure PIM Protocol is enabled in Global Mode (use ipv6 pim multicast-routing)
- ☞ Enable PIM-DM Protocol on the interface (use ipv6 pim dense-mode command)
- ☞ Multicast Protocol requires RPF Check using Unicast routing; therefore the correctness of Unicast routing must be assured beforehand

If all attempts including Check are made but the problems on PIM-DM can't be solved yet, then use debug commands such as debug pim please, and then copy DEBUG information in 3 minutes and send to Technology Service Center.

1.3 PIM-SM

1.3.1 Introduction to PIM-SM

PIM-SM（Protocol Independent Multicast, Sparse Mode）is Protocol Independent Multicast Sparse Mode. It is a Multicast Routing Protocol in Sparse Mode and mainly used in big scale network with group members distributed relatively sparse and wide-spread. Unlike the Flooding & Prune of Dense Mode, PIM-SM Protocol assumes no host needs receiving Multicast data packets. PIM-SM router transmits Multicast Data Packets to a host only if it presents explicit requirement.

By setting RP (Rendezvous Point) and BSR (Bootstrap Router), PIM-SM announce Multicast packet to all PIM-SM routers and establish RPT (RP-rooted shared tree) based on RP using Join/Prune message of routers. Consequently the network bandwidth occupied by data packets and message control is cut down and the transaction cost of routers decreases. Multicast data get to the network segment where the Multicast group members are located along the shared tree flow. When the data traffic reaches a certain amount, Multicast data stream can be switched to the shortest path tree SPT based on the source to reduce network delay. PIM-SM doesn't rely on any specific Unicast Routing Protocol but make RPF Check using existing Unicast routing table.

1. PIM-SM Working Principle

The central working processes of PIM-SM are: Neighbor Discovery, Generation of RP Shared Tree (RPT), Multicast source registration, SPT Switch, etc. We won't describe the mechanism of Neighbor Discovery here since it is same as that of PIM-DM.

(1) Generation of RP Shared Tree (RPT)

When a host joins a Multicast Group G, the leaf router that is connected to this host directly finds out through IGMP message that there is a receiver of Multicast Group G,

then it works out the corresponding Rendezvous Point RP for Multicast Group G, and send join message to upper lever nodes in RP direction. Every router on the way from the leaf router to RP will generate a (*, G) table entry, where a message from any source to Multicast group applies to this entry. When RP receives the message sent to Multicast Group G, the message will get to the leaf router along the set up path and reach the host. In this way the RPT with RP as root is generated.

(2) Multicast Source Registration

When a Multicast Source S sends a Multicast packet to Multicast Group G, the PIM-SM Multicast router connected to it directly will take charge of encapsulating the Multicast packet into registered message and unicast it to corresponding RP. If there are more than one PIM-SM Multicast routers on a network segment, then DR (Designated Router) takes charge of sending the Multicast packet.

(3) SPT Switch

When the Multicast router finds that the rate of the Multicast packet from RP with destination address G exceeds threshold, the Multicast router will send Join message to the next upper lever nodes in the source direction, which results in the switch from RPT to SPT.

2. Preparation before PIM-SM configuration

(1) Configuration Candidate RP

More than one RPs (candidate RP) can exist in PIM-SM network and each C-RP (Candidate RP) takes charge of transmitting Multicast packets with destination address in a certain range. To configure more than one candidate RPs can implement RP load share. No master or slave is differentiated among RPs. All Multicast routers work out the RP corresponding to some Multicast group based on the same algorithm after receiving the candidate RP message announced by BSR.

Note that one RP can serve more than one Multicast groups and all Multicast groups. Each Multicast group can only correspond to one unique RP at any moment. It can't correspond to more than one RP at the same time.

(2) Configure BSR

BSR is the management center of PIMSM network. It is in charge of collecting messages sent by candidate RPs and broadcast them.

Only one BSR can exist within a network, but more than one C-BSR (Candidate-BSR) can be configured. In this way, if some BSR goes wrong, it can switch to another. C-BSRs elect BSR automatically.

1.3.2 PIM-SM Configuration Task List

1. Enable PIM-SM (Required)
2. Configure static multicast routing entries (Optional)

3. Configure additional parameters for PIM-SM (Optional)
   (1) Configure parameters for PIM-SM interfaces
      1) Configure the interval for PIM-SM hello messages
      2) Configure the hold time for PIM-SM hello messages
      3) Configure ACL for PIM-SM neighbors
      4) Configure the interface as the boundary interface of the PIM-SM protocol
      5) Configure the interface as the management boundary of the PIM-SM protocol
   (2) Configure global PIM-SM parameters
      1) Configure the switch as a candidate BSR
      2) Configure the switch as a candidate RP
      3) Configure static RP
      4) Configure the cache time of kernel multicast route
4. Disable PIM-SM Protocol

1. Enable PIM-SM Protocol

The PIM-SM protocol can be enabled on Layer 3 switches by enabling PIM in global configuration mode and then enabling PIM-SM for specific interfaces in the interface configuration mode.

Command	Explanation
Global Mode	
ip pim multicast-routing	To enable the PIM-SM protocol for all the interfaces (However, in order to make PIM-SM work for specific interfaces, the following command should be issued).(Required)

And then turn on PIM-SM switch on the interface

Command	Explanation
Interface Configuration Mode	
ip pim sparse-mode	Enable PIM-SM Protocol of the interface. (Required).

2. Configure static multicast routing entries

Command	Explanation
Global Configuration Mode	
ip mroute <*A.B.C.D*> <*A.B.C.D*> <*ifname*> <*.ifname*> **no ip mroute <*A.B.C.D*> <*A.B.C.D*> [<*ifname*> <*.ifname*>]**	To configure a static multicast routing entry. The no form of this command will remove the specified static multicast routing entry.

3. Configure additional parameters for PIM-SM

(1) Configure parameters for PIM-SM interfaces

1) Configure the interval for PIM-SM hello messages

Command	Explanation
Interface Configuration Mode	
ip pim hello-interval <*interval*> **no ip pim hello-interval**	To configure the interval for PIM-SM hello messages. The no form of this command restores the interval to the default value.

2) Configure the hold time for PIM-SM hello messages

Command	Explanation
Interface Configuration Mode	
ip pim hello-holdtime <*value*> **no ip pim hello-holdtime**	To configure the value of the holdtime field in the PIM-SM hello messages. The no form of this command will restore the hold time to the default value.

3) Configure ACL for PIM-SM neighbors

Command	Explanation
Interface Configuration Mode	
ip pim neighbor-filter{<*access-list-number*> } **no ip pim neighbor-filter{<*access-list-number*> }**	To configure ACL to filter PIM-SM neighbors. If session to the neighbor has been denied by ACL, then the sessions that have been set up will be discarded immediately and new sessions will not be set up.

4) Configure the interface as the boundary interface of the PIM-SM protocol

Command	Explanation
Interface Configuration Mode	
ip pim bsr-border **no ip pim bsr-border**	To configure the interface as the boundary of PIM-SM protocol. On the boundary interface, BSR messages will not be sent or received. The network connected the interface is considered as directly connected network. The no form of this command will remove the configuration.

5) Configure the interface as the management boundary of the PIM-SM protocol

Command	Explanation

Interface Configuration Mode	
ip pim scope-border <*1-99* > | <*acl_name*> **no ip pim scope-border**	To configure PIM-SM management boundary for the interface and apply ACL for the management boundary. With default settings, 239.0.0.0/8 is considered as the scope of the management group. If ACL is configured, then the scope specified by ACL permit command is the scope of the management group. acl_name should be standard IPv4 ACL name. The no form of this command will remove the configuration.

(2) Configure global PIM-SM parameter

1) Configure the switch as a candidate BSR

Command	Explanation
Global Configuration Mode	
ip pim bsr-candidate {vlan <*vlan-id*>| <*ifname*>}[<*mask-length*>][<*priority*>] **no ip pim bsr-candidate**	This command is the global candidate BSR configuration command, which is used to configure the information of PIM-SM candidate BSR so that it can compete for BSR router with other candidate BSR. The "**no ip pim bsr-candidate**" command cancels the configuration of BSR.

2) Configure the switch as a candidate RP

Command	Explanation
Global Configuration Mode	
ip pim rp-candidate { vlan <*vlan-id*>| lookback<*index*> <*ifname*>} [<*A.B.C.D*>][<*priority*>] **no ip pim rp-candiate**	This command is the global candidate RP configuration command, which is used to configure the information of PIM-SM candidate RP so that it can compete for RP router with other candidate RP. The "**no ip pim rp-candidate**" command cancels the configuration of RP.

3) Configure static RP

Command	Explanation
Global Configuration Mode	

ip pim rp-address <*A.B.C.D*> [<*A.B.C.D/M*>] **no ip pim rp-address <*A.B.C.D*> {<*all*>|<*A.B.C.D/M*>}**	The command is the multicast group configuration static RP of the globally or multicast address range. The no form of this command will remove the configuration for the static RP.

4) Configure the cache time of kernel multicast route

Command	Explanation
Global Configuration Mode	
ip multicast unresolved-cache aging-time <value> **no ip multicast unresolved-cache aging-time**	Configure the cache time of kernel multicast route, the no command restores the default value.

4. Disable PIM-SM Protocol

Command	Explanation
Interface Configuration Mode	
no ip pim sparse-mode | no ip pim multicast-routing(Global configuration mode)	To disable the PIM-SM protocol.

1.3.3 PIM-SM Configuration Examples

As shown in the following figure, add the Ethernet interfaces of SwitchA, SwitchB, SwitchC and SwitchD to corresponding VLAN, and enable PIM-SM Protocol on each VLAN interface.

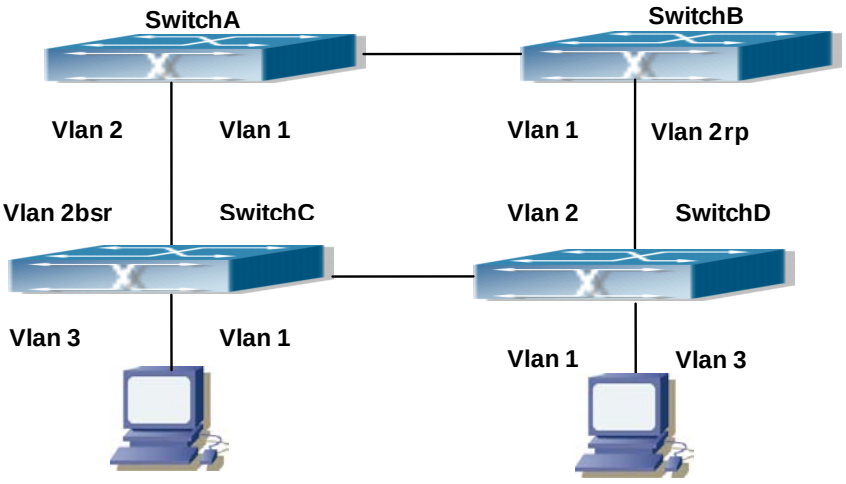


Fig 1-2 PIM-SM Typical Environment

The configuration procedure for SwitchA, SwitchB, SwitchC and SwitchD is as follows:

(1) Configure SwitchA:

```
Switch(config)#ip pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)# ip address 12.1.1.1 255.255.255.0
Switch(Config-if-Vlan1)# ip pim sparse-mode
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)# ip address 13.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)# ip pim sparse-mode
```

(2) Configure SwitchB:

```
Switch(config)#ip pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)# ip address 12.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)# ip pim sparse-mode
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)# ip address 24.1.1.2 255.255.255.0
Switch(Config-if-Vlan2)# ip pim sparse-mode
Switch(Config-if-Vlan2)# exit
Switch(config)# ip pim rp-candidate vlan2
```

(3) Configure SwitchC:

```
Switch(config)#ip pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)# ip address 34.1.1.3 255.255.255.0
Switch(Config-if-Vlan1)# ip pim sparse-mode
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)# ip address 13.1.1.3 255.255.255.0
Switch(Config-if-Vlan2)# ip pim sparse-mode
Switch(Config-if-Vlan2)#exit
Switch(config)#interface vlan 3
Switch(Config-if-Vlan3)# ip address 30.1.1.1 255.255.255.0
Switch(Config-if-Vlan3)# ip pim sparse-mode
Switch(Config-if-Vlan3)# exit
Switch(config)# ip pim bsr-candidate vlan2 30 10
```

(4) Configure SwitchD:

```
Switch(config)#ip pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)# ip address 34.1.1.4 255.255.255.0
Switch(Config-if-Vlan1)# ip pim sparse-mode
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)# ip address 24.1.1.4 255.255.255.0
Switch(Config-if-Vlan2)# ip pim sparse-mode
Switch(Config-if-Vlan2)#exit
Switch(config)#interface vlan 3
Switch(Config-if-Vlan3)# ip address 40.1.1.1 255.255.255.0
Switch(Config-if-Vlan3)# ip pim sparse-mode
```

At the same time, you should pay attention to the configuration of Unicast Routing Protocol, assure that each device can communicate with each other in the network layer, and be able to implement dynamic routing update in virtue of Unicast Routing Protocol.

1.3.4 PIM-SM Troubleshooting

In configuring and using PIM-SM Protocol, PIM-SM Protocol might not operate normally caused by physical connection or incorrect configuration. Therefore, the user should pay attention to the following issues:

- ☞ Assure that physical connection is correct;
- ☞ Assure the Protocol of Interface and Link is UP (use show interface command);
- ☞ Assure that PIM Protocol is enabled in Global Mode (use ip pim multicast-routing);
- ☞ Assure that PIM-SM is configured on the interface (use ip pim sparse-mode);
- ☞ Multicast Protocol requires RPF Check using unicast routing; therefore the correctness of unicast routing must be assured beforehand;
- ☞ PIM-SM Protocol requires supports by RP and BSR, therefore you should use show ip pim bsr-router first to see if there is BSR information. If not, you need to check if there is unicast routing leading to BSR.
- ☞ Use show ip pim rp-hash command to check if RP information is correct; if there is not RP information, you still need to check unicast routing.

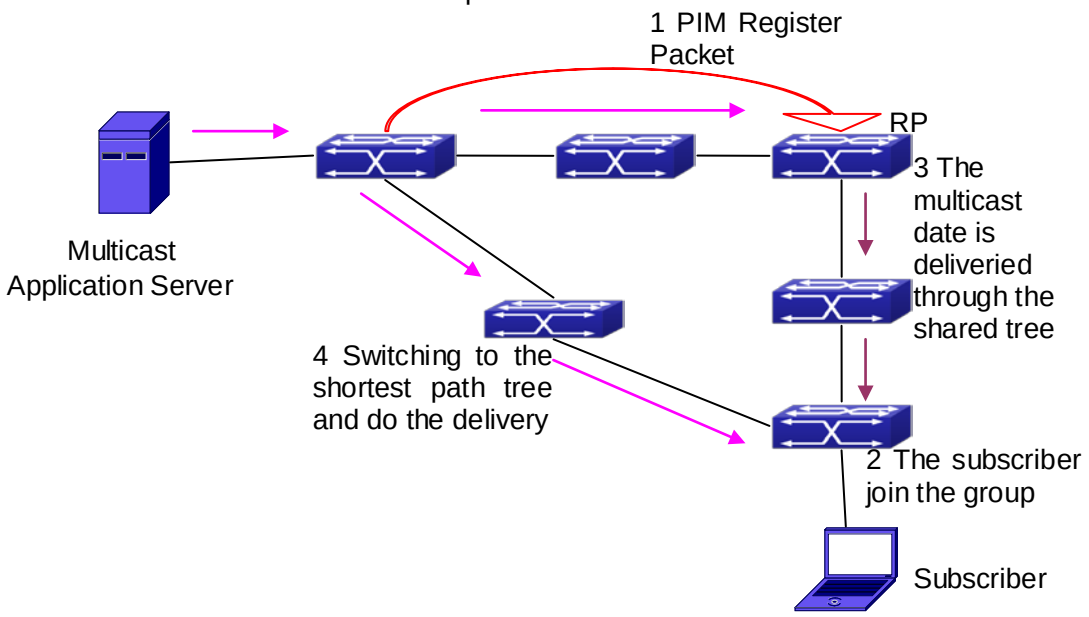
If all attempts including Check are made but the problems on PIM-SM can't be solved yet, then use debug commands such debug pim/debug pim BSR please, and then copy DEBUG information in 3 minutes and send to Technology Service Center.

1.4 MSDP Configuration

1.4.1 Introduction to MSDP

MSDP – Multicast Source Discovery Protocol, is a protocol that can learn information about multicast source in other PIM-SM domain. The RP on which MSDP is configured will advertise the information about the multicast sources in its domain to all the other MSDP entities through SA messages. Thus, all the information about multicast sources in one PIM-SM domain is spread to another. In MSDP, inter-domain information tree is used other than the shared tree. It is required that the multicast routing protocol used for in-domain routing must be PIM-SM.

☞ The work flow for RP in PIM-SM protocol



1.4.2 Brief Introduction to MSDP Configuration Tasks

1. Configuration of MSDP Basic Function
   1) Enabling MSDP (Required)
   2) Configuring MSDP entities (Required)
   3) Configuring the Connect-Source interface
   4) Configuring static RPF entities
   5) Configuring Originator RP
   6) Configuring TTL value
2. Configuration of MSDP entities

1) Configuring the Connect-Source interface
2) Configuring the descriptive information for MSDP entities
3) Configuring the AS number
4) Configuring the specified mesh group of MSDP
5) Configuring the maximum size for the cache

3. Configurations on delivery of SA packets
   1) Configuring filter policies for creation of SA packets
   2) Configuring filter rules on how to receive and forward SA packets
   3) Configuring SA request packets
   4) Configuring filter policies for SA-Request packets
4. Configuration of parameters of SA-cache
   1) Configuring SA packets cache
   2) Configuring the aging time for entries in SA packets cache
   3) Configuring the maximum size for the cache

1.4.3 Configuration of MSDP Basic Function

All the commands in this section are configured for RP in the PIM-SM domain. These RP will function as the other peer of the MSDP entities.

1.4.3.1 Prerequisites of MSDP Configuration

Before the MSDP basic functions can be configured, the following tasks should be done:

- At least one single cast routing protocol should be configured, in order to connect the network inside the domain and outside
- Configure PIM-SM in order to implement multicast inside the domain

When configuring MSDP basic function, the following information should be ready:

- The IP address of MSDP entities
- Filter policy table

Pay attention: MSDP can not use with Any-cast RP at same time, but configure Any-cast RP of based MSDP protocol.

1.4.3.2 Enabling MSDP

MSDP should be enabled before various MSDP functions can be configured.

1. Enable the MSDP function
2. Configure MSDP

1. Enabling MSDP

Commands	Explanation
Global Configuration Mode	
router msdp **no router msdp**	To enable MSDP. The no form of this command will disable MSDP globally.

2. Configuration of MSDP parameters

Commands	Explanation
MSDP Configuration Mode	
connect-source ***<interface-type>*** ***<interface-number>*** **no connect-source**	To configure the Connect-Source interface for MSDP Peer. The no form of this command will remove the configured Connect-Source interface.
default-rpf-peer ***<peer-address>*** ***[rp-policy <acl-list-number>|<word>]*** ***no*** **default-rpf-peer**	To configure static RPF Peer. The no form of this command will remove the configured RPF Peer.
originating-rp ***<interface-type>*** ***<interface-number>*** **no originating-rp**	To configure Originator-RP. The no form of this command will remove the configured Originator-RP.
ttl-threshold <*ttl*> **no ttl-threshold**	To configure the TTL value. The no form of this command will remove the configured TTL value.

1.4.4 Configuration of MSDP Entities

1.4.4.1 Creation of MSDP Peer

Commands	Explanation
MSDP Configuration Mode	
peer <*peer-address*> **no peer <*peer-address*>**	To create a MSDP Peer. The no form of this command will remove the configured MSDP Peer.

1.4.4.2 Configuration of MSDP parameters

Commands	Explanation

MSDP Peer Configuration Mode	
connect-source <*interface-type*> <*interface-number*> **no connect-source**	To configure the Connect-Source interface for MSDP Peer. The no form of this command will remove the configured Connect-Source interface.
description <*text*> **no description**	To configure the descriptive information about the MSDP entities. The no form of this command will remove the configured description.
remote-as <*as-num*> **no remote-as <*as-num*>**	To configure the AS number for MSDP Peer. The no form of this command will remove the configured AS number of MSDP Peer.
mesh-group <*name*> **no mesh-group <*name*>**	To configure an MSDP Peer to join the specified mesh group. The no form of this command will remove the MSDP Peer from the specified mesh group.

1.4.5 Configuration of Delivery of MSDP Packet

Commands	Explanation
MSDP Configuration Mode	
redistribute [list <*acl-list-number* |*acl-name*>] **no redistribute**	To configure the filter rules for creation of SA packets. The no form of this command will remove the configured.
MSDP Configuration Mode or MSDP Peer Configuration Mode	
sa-filter（in|out）[list <*acl-number* | *acl-name*> | rp-list <*rp-acl-number* | *rp-acl-name*>] **no sa-filter（in|out）[[list <*acl-number* | *acl-name*> | rp-list <*rp-acl-number* | *rp-acl-name*>]**	To configure the filter rules for receiving and forwarding SA packets. The no form of this command will remove the configured rules.
MSDP Peer Configuration Mode	
sa-request **no sa-request**	To configure sending of SA request packets. The no form of this command will disable sending of SA request packets.

MSDP Configuration Mode	
sa-request-filter [list <*access-list-number* | *access-list-name*>] **no sa-request-filter [list <*access-list-number* | *access-list-name*>]**	To configure filter rules for receiving SA request packets. The no form of this command will remove the configured filter rules for SA request packets.

1.4.6 Configuration of Parameters of SA-cache

Commands	Explanation
MSDP Configuration Mode	
cache-sa-state **no cache-sa-state**	To enable the SA packet cache. To disable the SA packets cache.
MSDP Configuration Mode	
cache-sa-holdtime <*150-3600*> **no cache-sa-holdtime**	The aging time for entries in the SA cache. To restore the default aging time configuration.
MSDP Configuration Mode or MSDP Peer Configuration Mode	
cache-sa-maximum <*sa-limit*> **no cache-sa-maximum**	To configure the maximum size for the SA cache. To restore the size of the SA cache to the default value.

1.4.7 MSDP Configuration Examples

Example 1: MSDP basic function.

Multicast Configuration:

1. Suppose the multicast server is sending multicast datagram at 224.1.1.1;
2. The designated router – DR, which is connected to the multicast server, encapsulate the multicast datagram in the Register packets and send them to the RP(RP1) in the local domain;
3. The RP unwraps the packets and sends them to all the domain members through the shared tree. The members in the domain can be configured to be or not to be in the shared tree;
4. At the same time, the source RP in the domain, generates a SA – Source Active message, and send it to the MSDP entity – RP2.
5. If there's another member in the same domain with the MSDP entity which is

named as RP3, RP3 will distribute the multicast datagram encapsulated in the SA messages to the members of the shared tree, and send join messages to the multicast source. That means RP creates an entry (S, G), and send join messages for (S, G) hop by hop, so that (S, G) can reach the SPT which takes the multicast source as the root across the PIM-SM domain.

If there no members in the same domain with MSDP entity – RP2, RP2 will not create the (S, G) entry nor it will join the SPT which takes the multicast source as the root.

6. When the reverse route has been set up, the multicast datagram from the source will be directly delivered to RP3, and RP will forward the datagram to the shared tree. At this time, the router which is closest to the domain members can determine itself whether or not to switch to SPT.

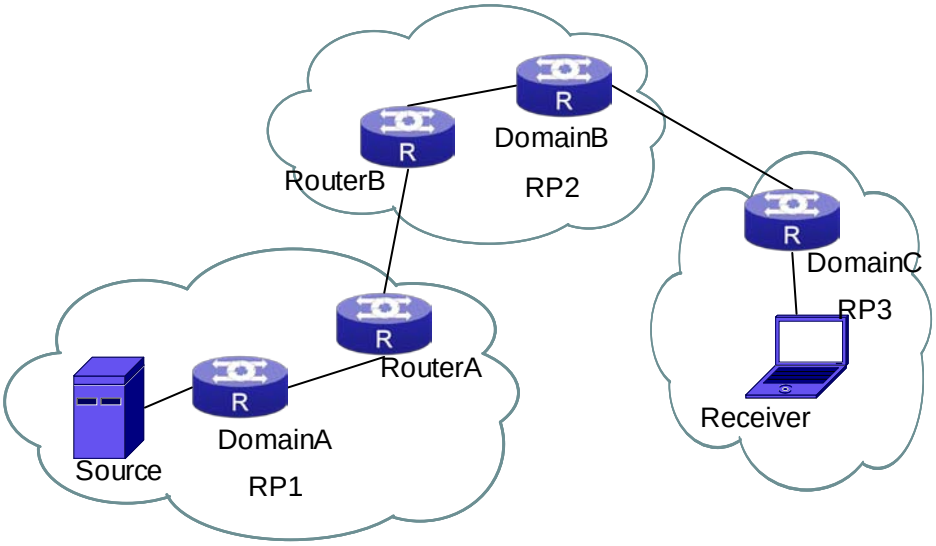


Fig 1-3 Network Topology for MSDP Entry

Configuration tasks are listed as below:

Prerequisites:

Enable the single cast routing protocol and PIM protocol on every router, and make sure that the inter-domain routing works well and multicasting inside the domain works well.

Suppose the multicast server S in Domain A offers multicast programs at 224.1.1.1. A host in Domain C named R subscribes this program. Before MSDP is configured C cannot subscribe the multicast program. However, with the following configuration, R is able to receive programs offered by S.

RP1 in Domain A:

```
Switch#config
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 10.1.1.2
```

Router A in Domain A:

```
Switch#config
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2    255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip address 20.1.1.2    255.255.255.0
Switch(Config-if-Vlan2)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 10.1.1.1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 20.1.1.1
```

Router B in Domain B:

```
Switch#config
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip address 20.1.1.1    255.255.255.0
Switch(Config-if-Vlan2)#exit
Switch(Config)#interface vlan 3
Switch(Config-if-Vlan3)#ip address 30.1.1.1    255.255.255.0
Switch(Config-if-Vlan3)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.2
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 30.1.1.2
```

RP2 in Domain B:

```
Switch#config
Switch(config)#interface vlan 3
Switch(Config-if-Vlan3)#ip address 30.1.1.2    255.255.255.0
Switch(config)#interface vlan 4
```

Switch(Config-if-Vlan4)#ip address 40.1.1.2 255.255.255.0
Switch(Config-if-Vlan4)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 30.1.1.1
Switch(config)#router msdp
Switch(router-msdp)#peer 40.1.1.1

RP3 in Domain C:

Switch(config)#interface vlan 4
Switch(Config-if-Vlan1)#ip address 40.1.1.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 40.1.1.2

Example 2: Application of MSDP Mesh-Group.

Mesh-Group can be used to reduce flooding of SA messages. The Peers which are meshed in the same domain can be configured as a Mesh-Group. All the members in the same mesh group use a unique group name.

As it is shown in Figure, when Mesh-Group is configured for the four meshed Peers in the same domain, flooding of SA messages reduced remarkably.

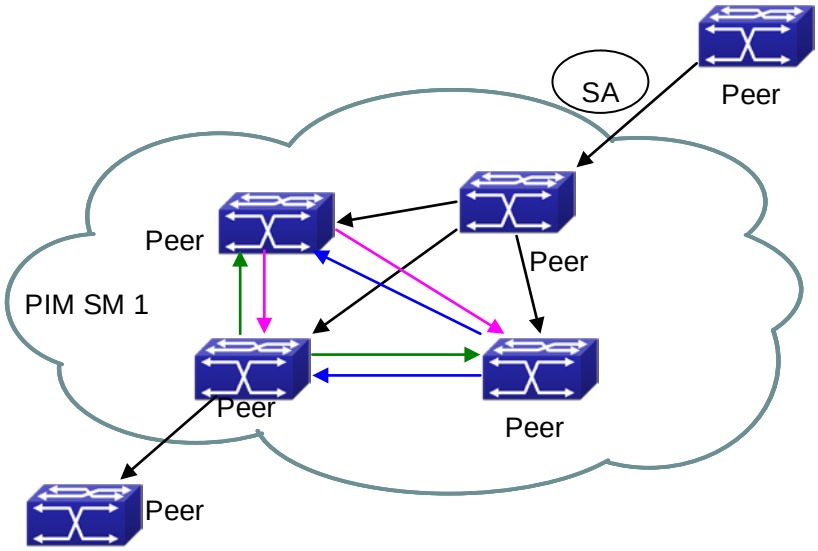


Fig 1-4 Flooding of SA messages

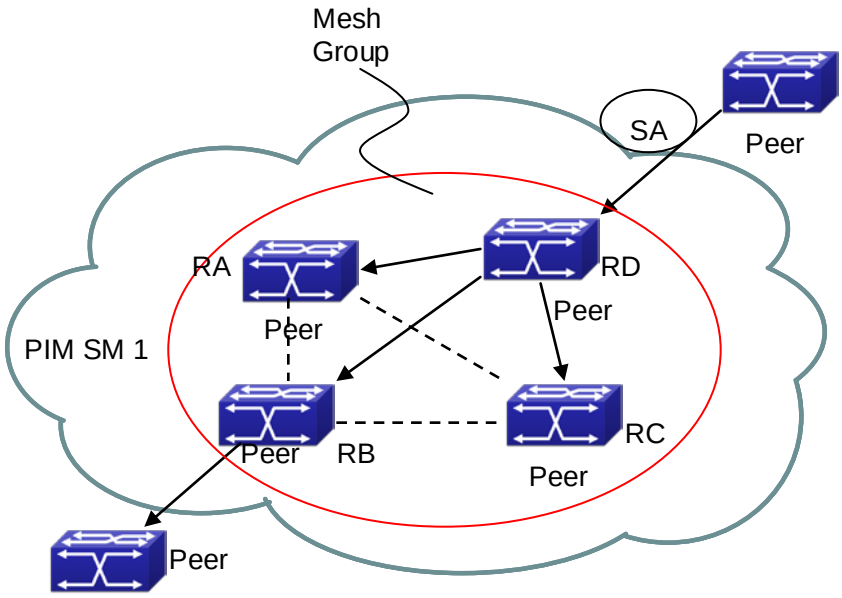


Fig 1-5 Flooding of SA messages with mesh group configuration

Configuration steps are listed as below:

Router A:

Switch#config
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip address 20.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)#exit
Switch(config)#interface vlan 3
Switch(Config-if-Vlan3)#ip address 30.1.1.1 255.255.255.0
Switch(Config-if-Vlan3)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 10.1.1.2
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 20.1.1.4
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 30.1.1.3
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit

Router B:

```
Switch#config
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.1.2  255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 4
Switch(Config-if-Vlan4)#ip address 40.1.1.2  255.255.255.0
Switch(Config-if-Vlan4)#exit
Switch(config)#interface vlan 6
Switch(Config-if-Vlan6)#ip address 60.1.1.2  255.255.255.0
Switch(Config-if-Vlan6)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 10.1.1.1
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 40.1.1.4
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 60.1.1.3
Switch(router-msdp)#mesh-group test-1
```

Router C:

```
Switch#config
Switch(config)#interface vlan 4
Switch(Config-if-Vlan4)#ip address 40.1.1.4  255.255.255.0
Switch(Config-if-Vlan4)#exit
Switch(config)#interface vlan 5
Switch(Config-if-Vlan5)#ip address 50.1.1.4  255.255.255.0
Switch(Config-if-Vlan5)#exit
Switch(config)#interface vlan 6
Switch(Config-if-Vlan6)#ip address 60.1.1.4  255.255.255.0
Switch(Config-if-Vlan6)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 40.1.1.4
```

Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 60.1.1.2
Switch(router-msdp)#mesh-group test-1

Router D:
Switch#config
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip address 20.1.1.4 255.255.255.0
Switch(Config-if-Vlan2)#exit
Switch(config)#interface vlan 4
Switch(Config-if-Vlan1)#ip address 40.1.1.4 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 5
Switch(Config-if-Vlan5)#ip address 50.1.1.4 255.255.255.0
Switch(Config-if-Vlan5)#exit
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 40.1.1.2
Switch(router-msdp)#mesh-group test-1
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 50.1.1.3
Switch(router-msdp)#mesh-group test-1

1.4.8 MSDP Troubleshooting

When MSDP is being configured, it may not function because of the physical link not working or configuration mistakes. Attention should be paid to the following items in order to make MSDP work:

- Make sure the physical link works well
- Make sure inner-domain and inter-domain routing works
- Make sure PIM-SM is applied in every domain as the inner-domain routing protocol, and configuration for PIM-SM works well
- Make sure MSDP is enabled, and the link status of the MSDP enabled Peer is UP
- Use the command **show msdp global** to check whether the MSDP configuration is correct

If the MSDP problems cannot be solved through all the methods provided above,

please issue the command **debug msdp** to get the debugging messages within three minutes, and send them to the technical service center of our company.

1.5 ANYCAST RP Configuration

1.5.1 Introduction to ANYCAST RP

Anycast RP is a technology based on PIM protocol, which provides redundancy in order to recover as soon as possible once an RP becomes unusable.

The kernel concept of Anycast RP is that the RP addresses configured all over the whole network exist on multiple multicast servers (the most common situation is that every device providing ANYCAST RP uses LOOPBACK interface, and using the longest mask to configures RP addresses on this interface), while the unicast routing algorithm will make sure that PIM routers can always find the nearest RP, thus , providing a shorter and faster way to find RP in a larger network., Once an RP being used becomes unusable, the unicast routing algorithm will ensure that the PIM router can find a new RP path fast enough to recover the multicast server in time. Multiple RP will cause a new problem that is if the multicast source and the receivers are registered to different RP, some receivers will not be able to receive data of multicast source (obviously, the register messages only prefer the nearest RP). So, in order to keep the communication between all RP, Anycast RP defines that the nearest RP to the multicast source should forward the source register messages to all the other RP to guarantee that all joiners of the RP can find the multicast source.

The method to realize the PIM-protocol-based Anycast RP is that: maintaining an ANYCAST RP list on every switch configured with Anycast RP and using another address as the label to identify each other. When one Anycast RP device receives a register message, it will send the register message to other Anycast RP devices while using its own address as the source address, to notify all the other devices of the original destination.

1.5.2 ANYCAST RP Configuration Task

1. Enable ANYCAST RP v4 function
2. Configure ANYCAST RP v4

1. Enable ANYCAST RP v4 function

Command	Explanation

Global Configuration Mode	
ip pim anycast-rp **no ip pim anycast-rp**	Enable ANYCAST RP function. (necessary) No operation will globally disable ANYCAST RP function.

2. Configure ANYCAST RP v4

(1) Configure the RP candidate

Command	Explanation
Global Configuration Mode	
ip pim rp-candidate {vlan<*vlan-id*> |loopback<*index*> |<*ifname*>} [<*A.B.C.D*>] [<*priority*>] **no ip pim rp-candidate**	Now, the PIM-SM has allowed the Loopback interface to be a RP candidate.(necessary) Please pay attention to that, ANYCAST RP protocol can configure the Loopback interface or a regular three-layer VLAN interface to be the RP candidate. In make sure that PIM routers in the network can find where the RP locates, the RP candidate interface should be added into the router. No operation will cancel the RP candidate configuration on this router.

(2) Configure self-rp-address (the RP address of this router)

Command	Explanation
Global Configuration Mode	
ip pim anycast-rp self-rp-address A.B.C.D **no ip pim anycast-rp self-rp-address**	Configure the self-rp-address of this router (as a RP). This address can be used to exclusively identify this router when communicating with other RP. the effect of **self-rp-address** refers to two respects: 1 Once this router (as a RP) receives the register message from DR unicast, it needs to forward the register message to all the other RP in the network, notifying them of the state of source (S.G). While forwarding the register message, this router will

	change the source address of it into self-rp-address. 2 Once this router(as a RP) receives a register message from other RP unicast, such as a register message whose destination is the self-rp-address of this router, it will create (S,G) state and send back a register-stop message, whose destination address is the source address of the register message. Pay attention: self-rp-address has to be the address of a three-layer interface on this router, but the configuration is allowed to be done with the absence of the interface. The self-rp-address should be unique. No operation will cancel the self-rp-address which is used to communicate with other RPs by this router (as a RP).

(3) Configure other-rp-address (other RP communication addresses)

Command	Explanation
Global Configuration Mode	
ip pim anycast-rp <*anycast-rp-addr*> <*other-rp-addr*> **no ip pim anycast-rp <*anycast-rp-addr*> <*other-rp-addr*>**	Configure anycast-rp-addr on this router (as a RP). This unicast address is actually the RP address configured on multiple RP in the network, in accordance with the address of RP candidate interface (or Loopback interface). The effect of **anycast-rp-addr** includes: 1 Although more than one anycast-rp-addr addresses are allowed to be configured, only the one having the same address with the currently configured RP candidate address will take effect. Only after that, can the other-rp-address in accordance with this anycast-rp-addr take effect. 2 The configuration is allowed to be done with the absence of the interface in

	accordance with the anycast-rp-addr. Configure on this router (as a RP) the other-rp-addresses of other RP communicating with it. This unicast address identifies other RP and is used in the communication with local routers. The effect of **other-rp-address** refers to two respects: 1 Once this router (as a RP) receives the register message from a DR unicast, it should forward it to other RP in the network to notify all the RP in the network of the source (S.G) state. While forwarding, the router will change the destination address of the register message into other-rp-address. 2 Multiple other-rp-addresses can be configured in accordance with one anycast-rp-addr, Once the register message from a DR is received, it should be forwarded to all of these other RP one by one. No operation will cancel an other-rp-address communicating with this router.

1.5.3 ANYCAST RP Configuration Examples

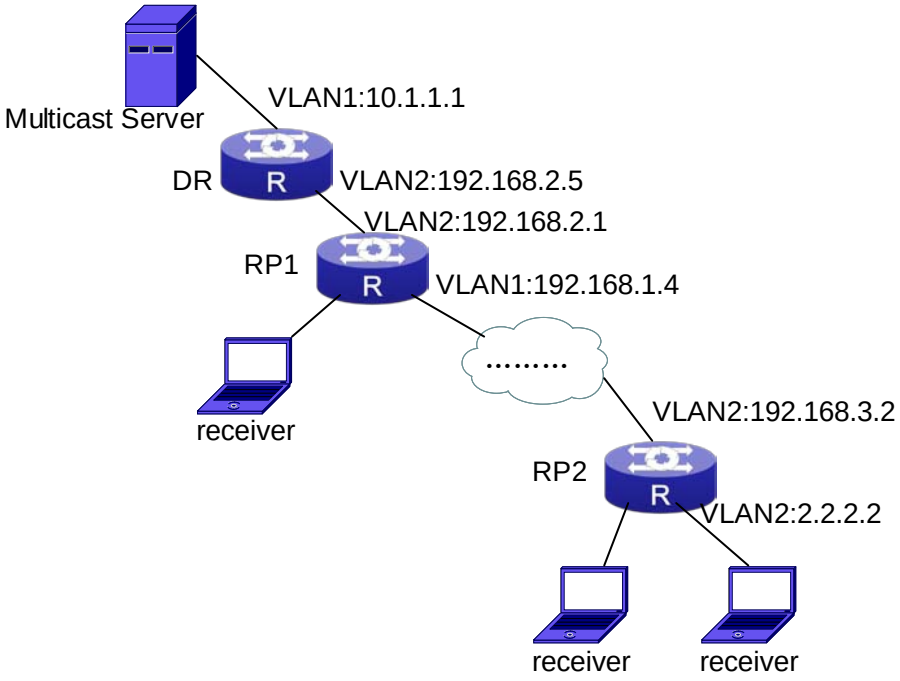


Fig 1-6 The ANYCAST RP v4 function of the router

As shown in the Figure, the overall network environment is PIM-SM, which provides two routers supporting ANYCAST RP, RP1 and RP2. Once multicast data from the multicast source server reaches the DR, the DR will send a multicast source register message to the nearest RP unicast according to the unicast routing algorithm, which is RP1 in this example. When RP1 receives the register message from the DR, besides redistributing to the shared tree according to the orderers who already join it, it will forward the multicast register message to RP2 to guarantee that all orders that already join RP2 can find the multicast source. Since there is an ANYCAST list maintained on router RP1 that has been configured with ANYCAST RP, and since this list contains the unicast addresses of all the other RP in the network, when the RP1 receives the register message, it can use the self-r-address, which identifies itself as the source address to forward the register message to RP2. The cloud in the Figure represents the PIM-SM network operation between RP1 and RP2.

The following is the configuration steps:

RP1 Configuration:

Switch#config

Switch(config)#interface loopback 1

Switch(Config-if-Loopback1)#ip address 1.1.1.1 255.255.255.255

Switch(Config-if-Loopback1)#exit

Switch(config)#ip pim rp-candidate loopback1

Switch(config)#ip pim bsr-candidate vlan 1

Switch(config)#ip pim multicast-routing
Switch(config)#ip pim anycast-rp
Switch(config)#ip pim anycast-rp self-rp-address 192.168.2.1
Switch(config)#ip pim anycast-rp 1.1.1.1 192.168.3.2

RP2 Configuration:

Switch#config
Switch(config)#interface loopback 1
Switch(Config-if-Loopback1)#ip address 1.1.1.1 255.255.255.255
Switch(Config-if-Loopback1)#exit
Switch(config)#ip pim rp-candidate loopback1
Switch(config)#ip pim multicast-routing
Switch(config)#ip pim anycast-rp
Switch(config)#ip pim anycast-rp self-rp-address 192.168.3.2
Switch(config)#ip pim anycast-rp 1.1.1.1 192.168.2.1

1.5.4 ANYCAST RP Troubleshooting

When configuring and using ANYCAST RP function, the ANYCAST RP might work abnormally because of faults in physical connections, configurations or something others. So, the users should pay attention to the following points:

- The physical connections should be guaranteed to be correct
- The PIM-SM protocol should be guaranteed to operate normally
- The ANYCAST RP should be guaranteed to be enabled in Global configuration mode
- The self-rp-address should be guaranteed to be configured correctly in Global configuration mode
- The other-rp-address should be guaranteed to be configured correctly in Global configuration mode
- All the interface routers should be guaranteed to be correctly added, including the loopback interface as a RP
- Use "**show ip pim anycast rp status**" command to check whether the configuration information of ANYCAST RP is correct

If the problems of ANYCAST still cannot be solved after checking, please use debug commands like "**debug pim anycast-rp**", then copy the DEBUG information within three minutes and send it to the technical service center of our company.

1.6 PIM-SSM

1.6.1 Introduction to PIM-SSM

Source Specific Multicast (PIM-SSM) is a new kind of multicast service protocol. With PIM-SSM, a multicast session is distinguished by the multicast group address and multicast source address. In SSM, hosts can be added into the multicast group manually and efficiently like the traditional PIM-SM, but leave out the shared tree and RP management in PIM-SM. In SSM, SPT tree will be constructed with (S, G). G for the multicast group address and S for the source address of the multicast which sends datagram to G. (S, G) in a pair is named as a channel of SSM. SSM serves best for the application of multicast service which is from one station to many ones, for example, the network sports video channel, and the news channel. By default, the multicast group address of SSM is limited between 232.0.0.0 and 232.255.255.255. However this address range can be extended according to actual situations.

1.6.2 PIM-SSM Configuration Task List

Command	Explanation
Global Configuration Mode	
ip multicast ssm {default|range *<access-list-number >*} **no ip multicast ssm**	To configure the address range for pim-ssm. The no form command will disable the configuration.

1.6.3 PIM-SSM Configuration Examples

As the figure shows, ethernet interfaces from SwitchA, SwitchB, SwitchC, and SwitchD are configured to be in separate VLANs. And PIM-SSM is enabled globally by enabling the PIM-SM or PIM-DM protocol on the VLAN interfaces. Take PIM-SM for example.

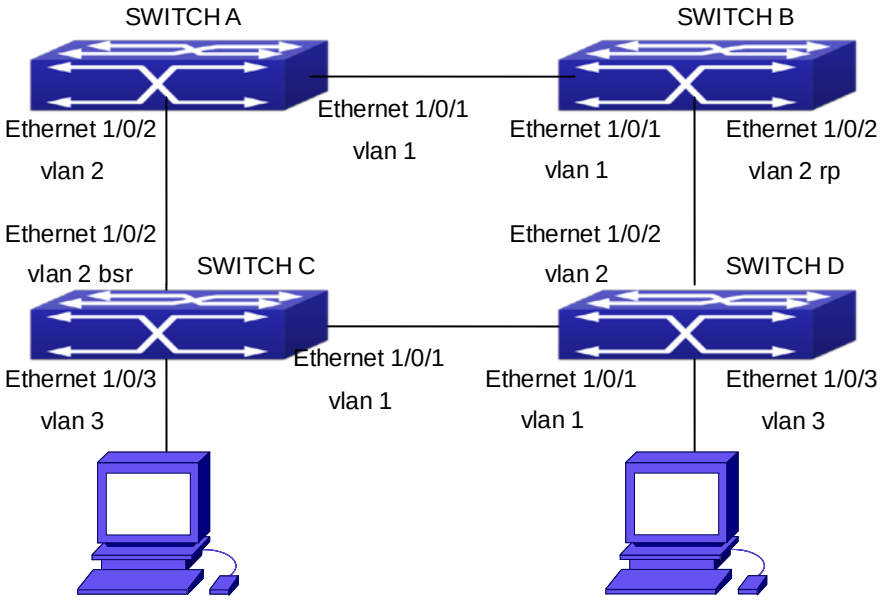


Fig 1-7 PIM-SSM typical environment

Configurations of SwitchA, SwitchB, SwitchC, and SwitchD are shown as below.

(1) Configuration of SwitchA.

Switch(config)#ip pim multicast-routing

Switch(config)#interface vlan 1

Switch(Config-If-Vlan1)# ip pim sparse-mode

Switch(Config-If-Vlan1)#exit

Switch(config)#interface vlan 2

Switch(Config-If-Vlan2)# ip pim sparse-mode

Switch(Config-If-Vlan2)#exit

Switch(config)#access-list 1 permit 224.1.1.1 0.0.0.255

Switch(config)#ip multicast ssm range 1

(2) Configuration of SwitchB.

Switch(config)#ip pim multicast-routing

Switch(config)#interface vlan 1

Switch(Config-If-Vlan1)# ip pim sparse-mode

Switch(Config-If-Vlan1)#exit

Switch(config)#interface vlan 2

Switch(Config-If-Vlan2)# ip pim sparse-mode

Switch(Config-If-Vlan2)# exit

Switch(config)# ip pim rp-candidate vlan2

Switch(config)#access-list 1 permit 224.1.1.1 0.0.0.255

Switch(config)#ip multicast ssm range 1
(3) Configuration of SwitchC.
Switch(config)#ip pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch(config)#interface vlan 3
Switch(Config-If-Vlan3)# ip pim sparse-mode
Switch(Config-If-Vlan3)# exit
Switch(config)# ip pim bsr-candidate vlan2 30 10
Switch(config)#access-list 1 permit 224.1.1.1 0.0.0.255
Switch(config)#ip multicast ssm range 1
(4) Configuration of SwitchD.
Switch(config)#ip pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch(config)#interface vlan 3
Switch(Config-If-Vlan3)# ip pim sparse-mode
Switch(Config-If-Vlan3)#exit
Switch(config)#access-list 1 permit 224.1.1.1 0.0.0.255
Switch(config)#ip multicast ssm range 1

1.6.4 PIM-SSM Troubleshooting

In configuring and using PIM-SSM Protocol, PIM-SSM Protocol might not operate normally caused by physical connection or incorrect configuration. Therefore, the user should pay attention to the following issues:

- Assure that physical connection is correct;
- Assure the Protocol of Interface and Link is UP (use **show interface** command);
- Assure that PIM Protocol is enabled in Global Mode (use **ip pim multicast-routing**);
- Assure that PIM-SSM is configured on the interface (use **ip pim sparse-mode**);

- ☞ Assure that SSM is configured in Global Mode;
- ☞ Multicast Protocol requires RPF check using unicast routing, therefore the correctness of unicast routing must be assured beforehand.

If all attempts including check are made but the problems on PIM-SSM can't be solved yet, then use debug commands such **debug pim event/debug pim packet** please, and then copy DEBUG information in 3 minutes and send to Technology Service Center.

1.7 DVMRP

1.7.1 Introduction to DVMRP

DVMRP Protocol, namely, is "Distance Vector Multicast Routing Protocol". It is a Multicast Routing Protocol in dense mode, which sets up a Forward Broadcast Tree for each source in a manner similar to RIP, and sets up a Truncation Broadcast Tree, i.e. the Shortest Path Tree to the source, for each source through dynamic Prune/Graft.

Some of the important features of DVMRP are:

1. The routing exchange used to determine reverse path checking information is based on distance vector (in a manner similar to RIP)
2. Routing exchange update occurs periodically (the default is 60 seconds)
3. TTL upper limit = 32 hops (and that RIP is 16)
4. Routing update includes net mask and supports CIDR

In comparison with Unicast routing, Multicast routing is a kind of reverse routing (that is, what you are interested in is where the packets are from but not where they go), thus the information in DVMRP routing table is used to determine if an input Multicast packet is received at the correct interface. Otherwise, the packet will be discarded to prevent Multicast circulation.

The check which determines if the packet gets to the correct interface is called RPF check. When some Multicast data packets get to some interface, it will determine the reverse path to the source network by looking up DVMRP router table. If the interface data packets get to is the one which is used to send Unicast message to the source, then the reverse path check is correct, and the data packets are forwarded out from all downstream interfaces. If not, then probably there is failure, and the Multicast packet is discarded.

Since not all switches support Multicast, DVMRP supports tunnel multicast communication, tunnel is a method to send multicast data report among DVMRP switches separated by switches which don't support multicast routing. Multicast data packets are encapsulated in unicast data packets and directly sent to the next switch which supports

multicast. DVMRP Protocol treats tunnel interface and general physical interface equally.

If two or more switches are connected to a multi-entrance network, it is likely to transmit more than one copy of a data packet to the sub-network. Thus a specified transmitter must be appointed. DVMRP achieves this goal by making use of routing exchange mechanism; when two switches on the multi-entrance network exchange routing information, they will be aware of the routing distance from each other to the source network, thus the switch with the shortest distance to the source network will become the specified transmitter of the sub-network. If some have the same distance, then the one with the lowest IP prevails.

After some interface of the switch is configured to Function DVMRP Protocol, the switch will multicast Probe message to other DVMRP switches on this interface, which is used to find neighbors and detect the capabilities of each other. If no Probe message from the neighbor is received until the neighbor is timed out, then this neighbor is considered missing.

In DVMRP, source network routing selection message are exchanged in a basic manner same to RIP. That is, routing report message is transmitted among DVMRP neighbors periodically (the default is 60 seconds). The routing information in DVMRP routing selection table is used to set up source distribution tree, i.e. to determine by which neighbor it passes to get to the source transmitting multicast packet; the interface to this neighbor is called upstream interface. The routing report includes source network (use net mask) address and the hop entry for routing scale.

In order to finish transmission correctly, every DVMRP switch needs to know which downstream switches need to receive multicast packet from some specific source network through it. After receiving packets from some specific source, DVMRP switch firstly will broadcast these multicast packets from all downstream interfaces, i.e. the interfaces on which there are other DVMRP switches which have dependence on the specific source. After receiving Prune message from some downstream switch on the interface, it will prune this switch. DVMRP switch uses poison reverse to notify the upstream switch for some specific source: “I am your downstream.” By adding infinity (32) to the routing distance of some specific source it broadcasts, DVMRP switch responds to the source upstream exchange to fulfill poison reverse. This means distance correct value is 1 to 2* infinity (32) -1 or 1 to 63, 1 to 63 means it can get to source network, 32 means source network is not arrival, 33 to 63 means the switch which generates the report message will receive multicast packets from specific source depending on upstream router.

1.7.2 DVMRP Configuration Task List

1. Globally enable and disable DVMRP (Required)
2. Configure Enable and Disable DVMRP Protocol at the interface (Required)

3. Configure DVMRP Sub-parameters (Optional)

   Configure DVMRP interface parameters

   1) Configure the delay of transmitting report message on DVMRP interface and the message number each time it transmits
   2) Configure metric value of DVMRP interface
   3) Configure if DVMRP is able to set up neighbors with DVMRP routers which can not Prune/Graft

4. Configure DVMRP tunnel

1. Globally enable DVMRP Protocol

The basic configuration to function DVMRP routing protocol on Layer 3 switch is very simple. Firstly it is required to turn on DVMRP switch globally.

Command	Explanation
Global Mode	
[no] ip dvmrp multicast-routing	Globally enable DVMRP Protocol, the "**no ip dvmrp multicast-routing**" command disables DVMRP Protocol globally. (Required)

2. Enable DVMRP Protocol on the interface

The basic configuration to function DVMRP routing protocol on Layer 3 switch is very simple. After globally enabling DVMRP Protocol, it is required to turn on DVMRP switch under corresponding interface.

Command	Explanation
Interface Configuration Mode	
ip dvmrp **no ip dvmrp**	Enable DVMRP Protocol on the interface, the "**no ip dvmrp**" command disables DVMRP Protocol on the interface.

3. Configure DVMRP Sub-parameters

（1）Configure DVMRP Interface Parameters

   1) Configure the delay of transmitting report message on DVMRP interface and the message number each time it transmits
   2) Configure metric value of DVMRP interface
   3) Configure if DVMRP is able to set up neighbors with DVMRP routers which can not Prune/Graft

Command	Explanation
Interface Configuration Mode	

ip dvmrp output-report-delay <*delay_val*> [<*burst_size*>] **no ip dvmrp output-report-delay**	Configure the delay of transmitting DVMRP report message on interface and the message number each time it transmits, the "**no ip dvmrp output-report-delay**" command restores default value.
ip dvmrp metric <*metric_val*> **no ip dvmrp metric**	Configure interface DVMRP report message metric value; the "**no ip dvmrp metric**" command restores default value.
ip dvmrp reject-non-pruners **no ip dvmrp reject-non-pruners**	Configure the interface rejects to set up neighbor relationship with non pruning/grafting DVMRP router. The "**no ip dvmrp reject-non-pruners**" command restores to being able to set up neighbor ship.

4. Configure DVMRP Tunnel

Command	Explanation
Interface Configuration Mode	
ip dvmrp tunnel <*index*> <*src-ip*> <*dst-ip*> **no ip dvmrp tunnel {<*index*> |<*src-ip*> <*dst-ip*>}**	This command configures a DVMRP tunnel; the "**no ip dvmrp tunnel {<*index*> |<*src-ip*> <*dst-ip*>}**" command deletes a DVMRP tunnel.

1.7.3 DVMRP Configuration Examples

As shown in the following figure, add the Ethernet interfaces of Switch A and Switch B to corresponding VLAN, and enable DVMRP on each VLAN interface.

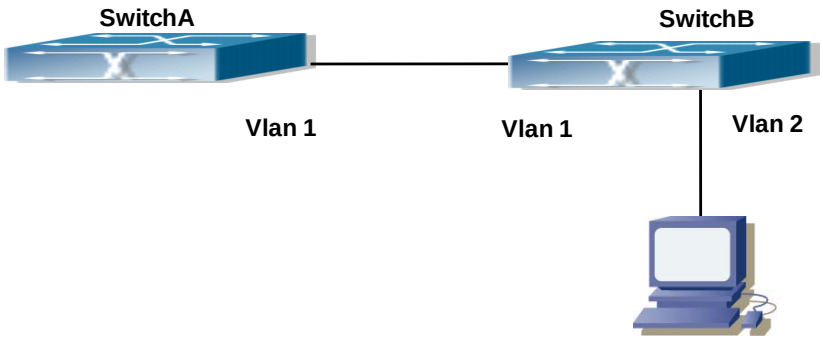


Fig 1-8 DVMRP Network Topology Diagram

The configuration procedure for SwitchA and SwitchB is as follows:

(1) Configure SwitchA:

Switch (config)#ip dvmrp multicast-routing

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)# ip address 10.1.1.1 255.255.255.0

Switch(Config-if-Vlan1)# ip dvmrp enable

(2) Configure SwitchB:

Switch (config)#ip dvmrp multicast-routing

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)# ip address 12.1.1.2 255.255.255.0

Switch(Config-if-Vlan1)# ip dvmrp enable

Switch(Config-if-Vlan1)#exit

Switch (config)#interface vlan 2

Switch(Config-if-Vlan2)# ip address 20.1.1.1 255.255.255.0

Switch(Config-if-Vlan2)# ip dvmrp

Since DVMRP itself does not rely on Unicast Routing Protocol, it is not necessary to configure Unicast Routing Protocol. This is the difference from PIM-DM and PIM-SM.

1.7.4 DVMRP Troubleshooting

In configuring and using DVMRP Protocol, DVMRP Protocol might not operate normally caused by physical connection or incorrect configuration. Therefore, the user should pay attention to the following issues:

- ☞ Firstly to assure that physical connection is correct;
- ☞ Next, to assure the Protocol of Interface and Link is UP (use **show interface** command);
- ☞ Please check if the correct IP address is configured on the interface (use **ip address** command);
- ☞ Afterwards, enable DVMRP Protocol on the interface (use **ip dvmrp** command and **ip dv multicast-routing** command);
- ☞ Multicast Protocol requires RPF Check using unicast routing; therefore the correctness of unicast routing must be assured beforehand. (DVMRP uses its own unicast table, please use **show ip dvmrp route** command to look up).

If all attempts including Check are made but the problems on DVMRP can't be solved yet, then please use commands such as debug DVMRP, and then copy DEBUG information in 3 minutes and send to Technology Service Center.

1.8 DCSCM

1.8.1 Introduction to DCSCM

DCSCM (Destination control and source control multicast) technology mainly includes three aspects, i.e. Multicast Packet Source Controllable, Multicast User Controllable and Service-Oriented Priority Strategy Multicast.

The Multicast Packet Source Controllable technology of Security Controllable Multicast technology is mainly processed in the following manners:

1. On the edge switch, if source under-control multicast is configured, then only multicast data from specified group of specified source can pass.
2. For RP switch in the core of PIM-SM, for REGISTER information out of specified source and specified group, REGISTER_STOP is transmitted directly and table entry is not allowed to set up. (This task is implemented in PIM-SM model).

The implement of Multicast User Controllable technology of Security Controllable Multicast technology is based on the control over IGMP report message sent out by the user, thus the model being controlled is IGMP snooping and IGMPmodel, of which the control logic includes the following three, i.e. to take control based on VLAN+MAC address transmitting packets, to take control based on IP address of transmitting packets and to take control based on the port where messages enter, in which IGMP snooping can use the above three methods to take control simultaneously, while since IGMP model is located at layer 3, it only takes control over the IP address transmitting packets.

The Service-Oriented Priority Strategy Multicast of Security Controllable technology adopts the following mode: for multicast data in limit range, set the priority specified by the user at the join-in end so that data can be sent in a higher priority on TRUNK port, consequently guarantee the transmission is processed in user-specified priority in the entire network.

1.8.2 DCSCM Configuration Task List

1. Source Control Configuration
2. Destination Control Configuration
3. Multicast Strategy Configuration

1. Source Control Configuration

Source Control Configuration has three parts, of which the first is to enable source control. The command of source control is as follows:

Command	Explanation

Global Configuration Mode	
[no] ip multicast source-control (Required)	Enable source control globally, the "**no ip multicast source-control**" command disables source control globally. It is noticeable that, after enabling source control globally, all multicast packets are discarded by default. All source control configuration can not be processed until that it is enabled globally, while source control can not be disabled until all configured rules are disabled.

The next is to configure the rule of source control. It is configured in the same manner as for ACL, and uses ACL number of 5000-5099, every rule number can be used to configure 10 rules. It is noticeable that these rules are ordered, the front one is the one which is configured the earliest. Once the configured rules are matched, the following rules won't take effect, so rules of globally allow must be put at the end. The commands are as follows:

Command	Explanation
Global Configuration Mode	
[no] access-list <*5000-5099*> {deny|permit} ip {{<*source*> <*source-wildcard*>}|{host-source <*source-host-ip*>}|any-source} {{<*destination*> <*destination-wildcard*>}|{host-destination <*destination-host-ip*>}|any-destination}	The rule used to configure source control. This rule does not take effect until it is applied to specified port. Using the NO form of it can delete specified rule.

The last is to configure the configured rule to specified port.

Note: If the rules being configured will occupy the table entries of hardware, configuring too many rules will result in configuration failure caused by bottom table entries being full, so we suggest user to use the simplest rules if possible. The configuration rules are as follows:

Command	Explanation
Port Configuration Mode	
[no] ip multicast source-control access-group <*5000-5099*>	Used to configure the rules source control uses to port, the NO form cancels the configuration.

2. Destination Control Configuration

Like source control configuration, destination control configuration also has three steps.

First, enable destination control globally. Since destination control need to prevent unauthorized user from receiving multicast data, the switch won't broadcast the multicast data it received after configuring global destination control. Therefore, It should be avoided to connect two or more other Layer 3 switches in the same VLAN on a switch on which destination control is enabled. The configuration commands are as follows:

Command	Explanation
Global Configuration Mode	
[no] multicast destination-control（required）	Globally enable IPv4 and IPv6destination control. The no operation of this command will globally disable destination control. All of the other configuration can only take effect after globally enabled. The next is configuring destination control rules, which are similar.

Next is to configure the multicast destination control profile rule list and use the profile-id number of 1-50.

Command	Explanation
Global Configuration Mode	
profile-id <1-50> {deny|permit} {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination} **no profile-id <1-50>**	Configure the destination control profile rule. The no command deletes it.

Then configure destination control rule. It is similar to source control, except to use ACL No. of 6000-7999.

Command	Explanation
Global Configuration Mode	

[no] access-list <6000-7999> {{{add | delete} profile-id WORD} | {{deny|permit} (ip) {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination}}	The rule used to configure destination control. This rule does not take effect until it is applied to source IP or VLAN-MAC and port. Using the NO form of it can delete specified rule.

The last is to configure the rule to specified source IP, source VLAN MAC or specified port. It is noticeable that, due to the above situations, these rules can only be used globally in enabling IGMP-SNOOPING. And if IGMP-SNOOPING is not enabled, then only source IP rule can be used under IGMP Protocol. The configuration commands are as follows:

Command	Explanation
Port Configuration Mode	
[no] ip multicast destination-control access-group <*6000-7999*>	Used to configure the rules destination control uses to port, the NO form cancels the configuration.
Global Configuration Mode	
[no] ip multicast destination-control <*1-4094*> <*macaddr*> access-group <6000-7999>	Used to configure the rules destination control uses to specify VLAN-MAC, the NO form cancels the configuration.
[no] ip multicast destination-control <*IPADDRESS/M*> access-group <*6000-7999*>	Used to configure the rules destination control uses to specified IP address/net mask, the NO form cancels the configuration.

3. Multicast Strategy Configuration

Multicast Strategy uses the manner of specifying priority for specified multicast data to achieve and guarantee the effects the specific user requires. It is noticeable that multicast data can not get a special care all along unless the data are transmitted at TRUNK port. The configuration is very simple, it has only one command, i.e. to set priority for the specified multicast. The commands are as follows:

Command	Explanation
Global Configuration Mode	

[no] ip multicast policy <*IPADDRESS/M*> <*IPADDRESS/M*> cos <*priority*>	Configure multicast strategy, specify priority for sources and groups in specific range, and the range is <0-7>.

1.8.3 DCSCM Configuration Examples

1. Source Control

In order to prevent an Edge Switch from putting out multicast data ad asbitsium, we configure Edge Switch so that only the switch at port Ethernet1/0/5 is allowed to transmit multicast, and the data group must be 225.1.2.3. Also, switch connected up to port Ethernet1/0/10 can transmit multicast data without any limit, and we can make the following configuration.

EC(config)#access-list 5000 permit ip any host 225.1.2.3

EC(config)#access-list 5001 permit ip any any

EC(config)#ip multicast source-control

EC(config)#interface ethernet1/0/5

EC(Config-If-Ethernet1/0/5)#ip multicast source-control access-group 5000

EC(config)#interface ethernet1/0/10

EC(Config-If-Ethernet1/0/10)#ip multicast source-control access-group 5001

2. Destination Control

We want to limit users with address in 10.0.0.0/8 network segment from entering the group of 238.0.0.0/8, so we can make the following configuration:

Firstly enable IGMP snooping in the VLAN it is located (Here it is assumed to be in VLAN2)

EC(config)#ip igmp snooping

EC(config)#ip igmp snooping vlan 2

After that, configure relative destination control access-list, and configure specified IP address to use that access-list.

Switch(config)#access-list 6000 deny ip any 238.0.0.0 0.255.255.255

Switch(config)#access-list 6000 permit ip any any

Switch(config)#multicast destination-control

Switch(config)#ip multicast destination-control 10.0.0.0/8 access-group 6000

In this way, users of this network segment can only join groups other than 238.0.0.0/8.

Or configure the destination control access-list by adding the profile list.

Switch (config)#profile-id 1 deny ip any 238.0.0.0 0.255.255.255

Switch (config)#access-list 6000 add profile-id 1

Switch (config)#multicast destination-control

Switch (config)#ip multicast destination-control 10.0.0.0/8 access-group 6000

3. Multicast strategy

Server 210.1.1.1 is distributing important multicast data on group 239.1.2.3, we can configure on its join-in switch as follows:

Switch(config)#ip multicast policy 210.1.1.1/32 239.1.2.3/32 cos 4

In this way, the multicast stream will have a priority of value 4 (Usually this is pretty higher, the higher possible one is protocol data; if higher priority is set, when there is too many multicast data, it might cause abnormal behavior of the switch protocol) when it gets to other switches through this switch.

1.8.4 DCSCM Troubleshooting

The effect of DCSCM module itself is similar to ACL, and the problems occurred are usually related to improper configuration. Please read the descriptions above carefully. If you still can not determine the cause of the problem, please send your configurations and the effects you expect to the after-sale service staff of our company.

1.9 IGMP

1.9.1 Introduction to IGMP

IGMP (Internet Group Management Protocol) is the protocol in TCP/IP protocol family which is responsible for IP multicast member management. It is used to set up and maintain multicast group member relationship between IP host and its neighbor multicast switches. IGMP does not include the spread and maintenance of relation information of group members among multicast switches, this work is accomplished by each multicast routing protocol. All hosts participating in multicast must implement IGMP protocol.

Hosts participating IP multicast can join in and exit multicast group at any location, any time and without limit of member total. Multicast switch does not need and not likely to save all relationships of all hosts. It only gets to know if there are receivers of some multicast group, i.e. group member, on the network segment each interface connects to. And the host only needs to save which multicast groups it joined.

IGMP is asymmetric between host and router: the host needs to respond the IGMP query messages of multicast switches, i.e. to report message response in membership; the switch sends out membership query messages periodically, and then determine if there are hosts of some specific group joining in the sub-network it belongs to based on the received response message, and send out query of specific group (IGMP version2)

when receiving the report of a host exiting the group to determine if there exists no member in some specific group.

Up to now, there are three versions of IGMP: IGMP version1 (defined by RFC1112), IGMP version2 (defined by RFC2236) and IGMP version3 (defined by RFC3376).

The main improvements of IGMP version2 over version1 are:

1. The election mechanism of multicast switches on the shared network segment

Shared network segment is the situation of there is more than one multicast switch on a network segment. Under this kind of situation, since all switches which runs IGMP under this network segment can get membership report message from the host, therefore, only one switch is required to transmit membership query message, so an exchange election mechanism is required to determine a switch as query machine. In IGMP version1, the selection of query machine is determined by Multicast Routing Protocol; IGMP version2 made an improvement for it, it prescribed that when there are more than one multicast switches on the same network segment, the multicast switch with the lowest IP address will be elected as the query machine.

2. IGMP version2 added Leave Group Mechanism

In IGMP version 1, the host leaves the multicast group silently without sending any notification to any multicast switch. This causes that the multicast switch can only determine the leave of multicast member by multicast group response time-out. But in version2, when a host decides to leave a multicast group, if it is the host which gives response to the latest membership query message, then it will send out a message implying it is leaving.

3. IGMP version 2 added the query to specific group

In IGMP version1, a query of multicast switch is for all multicast groups on the network segment. This query is called general group query. In IGMP version2, query of specific group is added besides general group query. The destination IP address of this kind of query message is the IP address of the multicast group, the group address field part of the message is also the IP address of the multicast group. Thus it is prevented that hosts which are other multicast group members transmit response message.

4. IGMP version2 added the biggest response time field

IGMP version2 added the biggest response time field to dynamically adjust the response time of the host to group query message.

The main features of version3 is allowing the host to choose receiving from or rejecting a certain source, which is the basis of SSM（Source-Specific Multicast）multicast. For example, when a host is sending a report of INCLUDE{10.1.1.1, 10.1.1.2} to some group G, that means the host needs the router to forward the flux from 10.1.1.1 and 10.1.1.2; when a host is sending a report of EXCLUDE{192.168.1.1} to some group G,

that means the host needs the flux from all sources of group G except 192.168.1.1. This makes a great difference from the previous IGMP.

The main improvements of IGMP Version3 over IGMP Version1 and Version2 are:

1. The status to be maintained is group and source list, not only the groups in IGMPv2.
2. The interoperations with IGMPv1 and IGMPv2 are defined in IGMPv3 status.
3. IP service interface is modified to allow specific source list thereby.
4. The queried includes his/her Robustness Variable and Query Interval in query group to allow the synchronization with these variables of non-queries.
5. Max Response Time in Query Message has an exponential range, with maximum value from 25.5 secs of v2 to 53 mins, which can be used in links of great capacity.
6. In order to increase strength, the host retransmits State-Change message.
7. Additional data is defined to adapt future extension.
8. Report group is sent to 224.0.0.22 to help with IGMP Snooping of Layer 2 Switch.
9. Report group can include more than one group record, and it allows using small group to report complete current status.
10. The host does not restrain operation any more, which simplifies the implement and allows direct membership trace.
11. In querying messages, the new router side restraint process (S sign) modified the existing strength of IGMPv2.

1.9.2 IGMP Configuration Task List

1. Enable IGMP (Required)
2. Configure IGMP sub-parameters (Optional)
   （1）Configure IGMP group parameters
      1) Configure IGMP group filtering conditions
      2) Configure IGMP to join in group
      3) Configure IGMP to join in static group
   （2）Configure IGMP query parameters
      1) Configure the interval of IGMP sending query message
      2) Configure the maximum response time of IGMP query
      3) Configure time-out of IGMP query
   （3）Configure IGMP version
3. Disable IGMP Protocol

1. Enable IGMP Protocol

There are not specific commands for enabling IGMP Protocol on the Layer 3 switch. Enabling any multicast protocol under corresponding interface will automatically enable IGMP.

Command	Explanation
Global Mode	
ip dvmrp multicast-routing | ip pim multicast-routing	To enable global multicast protocol is the prerequisite to enable IGMP protocol, the "**no ip dvmrp multicast-routing | no ip pim multicast-routing**" commands disable multicast protocol and IGMP protocol. (Required)

Command	Explanation
Interface Configuration Mode	
ip dvmrp enable| ip pim dense-mode | ip pim sparse-mode	Enable IGMP Protocol, the corresponding commands "**no ip dvmrp enable| no ip pim dense-mode | no ip pim sparse-mode**" disable IGMP Protocol. (Required)

2. Configure IGMP Sub-parameters

（1）Configure IGMP group parameters

1) Configure IGMP group filtering conditions
2) Configure IGMP to join in group
3) Configure IGMP to join in static group

Command	Explanation
Interface Configuration Mode	
ip igmp access-group {<*acl_num* | *acl_name*>} **no ip igmp access-group**	Configure the filtering conditions of the interface to IGMP group; the "**no ip igmp access-group**" command cancels the filtering condition.
ip igmp join-group <*A.B.C.D* > **no ip igmp join-group <*A.B.C.D* >**	Configure the interface to join in some IGMP group, the "**no ip igmp join-group <*A.B.C.D* >**" command cancels the join.
ip igmp static-group <*A.B.C.D* > **no ip igmp static-group <*A.B.C.D*>**	Configure the interface to join in some IGMP static group; the "**no ip igmp static-group <*A.B.C.D* >**" command cancels the join.

（2）Configure IGMP Query parameters

1) Configure interval for IGMP to send query messages
2) Configure the maximum response time of IGMP query
3) Configure the time-out of IGMP query

Command	Explanation

Interface Configuration Mode	
ip igmp query-interval <*time_val*> **no ip igmp query-interval**	Configure the interval of IGMP query messages sent periodically; the "**no ip igmp query-interval**" command restores default value.
ip igmp query-max-response-time <*time_val*> **no ip igmp query-max-response-time**	Configure the maximum response time of the interface for IGMP query; the "**no ip igmp query-max-response-time**" command restores default value.
ip igmp query-timeout <*time_val*> **no ip igmp query-timeout**	Configure the time-out of the interface for IGMP query; the "**no ip igmp query-timeout**" command restores default value.

（3）Config IGMP version

Command	Explanation
Global Mode	
ip igmp version <*version*> **no ip igmp version**	Configure IGMP version on the interface; the "**no ip igmp version**" command restores the default value.

3. Disable IGMP Protocol

Command	Explanation
Interface Configuration Mode	
no ip dvmrp | no ip pim dense-mode | no ip pim sparse-mode | no ip dvmrp multicast-routing | no ip pim multicast-routing	Disable IGMP Protocol.

1.9.3 IGMP Configuration Examples

As shown in the following figure, add the Ethernet ports of Switch A and Switch B to corresponding VLAN, and start PIM-DM on each VLAN interface.

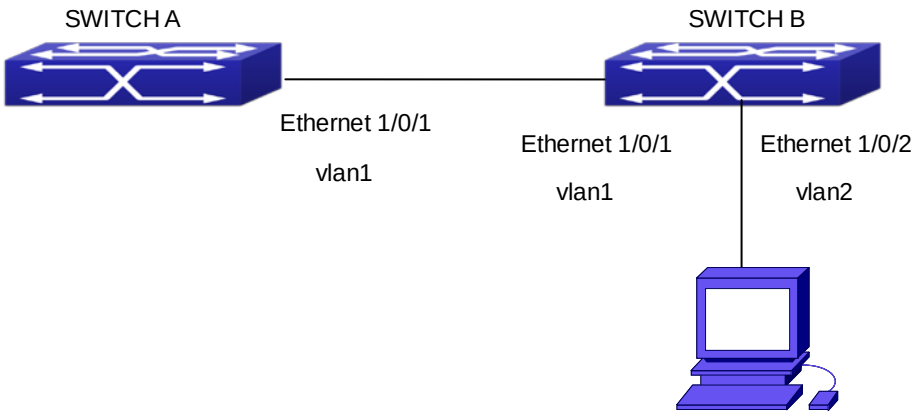


Fig 1-9 IGMP Network Topology Diagram

The configuration procedure for SwitchA and SwitchB is as follows:

(1) Configure SwitchA:

Switch(config)#ip pim multicast-routing

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip address 12.1.1.1 255.255.255.0

Switch(Config-if-Vlan1)#ip pim dense-mode

(2) Configure SwitchB:

Switch(config)#ip pim multicast-routing

Switch(config)#interface vlan1

Switch(Config-if-Vlan1)#ip address 12.1.1.2 255.255.255.0

Switch(Config-if-Vlan1)#ip pim dense-mode

Switch(Config-if-Vlan1)#exit

Switch(config)#interface vlan2

Switch(Config-if-Vlan1)#ip address 20.1.1.1 255.255.255.0

Switch(Config-if-Vlan2)#ip pim dense-mode

Switch(Config-if-Vlan2)#ip igmp version 3

1.9.4 IGMP Troubleshooting

In configuring and using IGMP Protocol, IGMP Protocol might not operate normally caused by physical connection or incorrect configuration. Therefore, user should pay attention to the following issues:

- Firstly to assure that physical connection is correct;
- Next, to assure the Protocol of Interface and Link protocol is UP (use show interface command);

- ☞ Afterwards, to assure to start a kind of multicast protocol on the interface;
- ☞ Multicast Protocol requires RPF Check using unicast routing; therefore the correctness of unicast routing must be assured beforehand.

1.10 IGMP Snooping

1.10.1 Introduction to IGMP Snooping

IGMP (Internet Group Management Protocol) is a protocol used in IP multicast. IGMP is used by multicast enabled network device (such as a router) for host membership query, and by hosts that are joining a multicast group to inform the router to accept packets of a certain multicast address. All those operations are done through IGMP message exchange. The router will use a multicast address (224.0.0.1) that can address to all hosts to send an IGMP host membership query message. If a host wants to join a multicast group, it will reply to the multicast address of that a multicast group with an IGMP host membership reports a message.

IGMP Snooping is also referred to as IGMP listening. The switch prevents multicast traffic from flooding through IGMP Snooping, multicast traffic is forwarded to ports associated to multicast devices only. The switch listens to the IGMP messages between the multicast router and hosts, and maintains multicast group forwarding table based on the listening result, and can then decide to forward multicast packets according to the forwarding table.

Switch provides IGMP Snooping and is able to send a query from the switch so that the user can use switch in IP multicast.

1.10.2 IGMP Snooping Configuration Task List

1. Enable IGMP Snooping
2. Configure IGMP Snooping

1. Enable IGMP Snooping

Command	Explanation
Global Mode	
ip igmp snooping **no ip igmp snooping**	Enables IGMP Snooping. The no operation disables IGMP Snooping function.

2. Configure IGMP Snooping

Command	Explanation
Global Mode	
ip igmp snooping vlan <*vlan-id*> **no ip igmp snooping vlan <*vlan-id*>**	Enables IGMP Snooping for specified VLAN. The no operation disables IGMP Snooping for specified VLAN.
ip igmp snooping proxy **no ip igmp snooping proxy**	Enable IGMP Snooping proxy function, the no command disables the function.
ip igmp snooping vlan < *vlan-id* > limit {group <*g_limit*> | source <*s_limit*>} **no ip igmp snooping vlan < *vlan-id* > limit**	Configure the max group count of vlan and the max source count of every group. The "no **ip igmp snooping vlan <*vlan-id*> limit"** command cancels this configuration.
ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit {group <1-65535>| source <1-65535>} strategy (replace | drop) **no ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit group source strategy**	Configure the number of groups which are allowed joining and the maximum of the source in each group under the IGMP Snooping port. Configure the strategy when it is up to the upper limit, including "replace" and "drop". No command configures as "no limitation".
ip igmp snooping vlan <*vlan-id*> l2-general-querier **no ip igmp snooping vlan <*vlan-id*> l2-general-querier**	Set this vlan to layer 2 general querier. It is recommended to configure a layer 2 general querier on a segment. The "no **ip igmp snooping vlan <*vlan-id*> l2-general-querier"command** cancels this configuration.
ip igmp snooping vlan <*vlan-id*> l2-general-querier-version <version>	Configure the version number of a general query from a layer 2 general querier.
ip igmp snooping vlan <*vlan-id*> l2-general-querier-source <source>	Configure the source address of a general query from a layer 2 general querier.
ip igmp snooping vlan <*vlan-id*> mrouter-port interface <*interface –name*> **no ip igmp snooping vlan <*vlan-id*> mrouter-port interface <*interface –name*>**	Configure static mrouter port of vlan. The no form of the command cancels this configuration.

ip igmp snooping vlan <*vlan-id*> mrouter-port learnpim **no ip igmp snooping vlan <*vlan-id*> mrouter-port learnpim**	Enable the function that the specified VLAN learns mrouter-port (according to pim packets), the no command will disable the function.
ip igmp snooping vlan <*vlan-id*> mrpt <*value* > **no ip igmp snooping vlan <*vlan-id*> mrpt**	Configure this survive time of mrouter port. The "no **ip igmp snooping vlan <*vlan-id*> mrpt"** command restores the default value.
ip igmp snooping vlan <*vlan-id*> query-interval <*value*> **no ip igmp snooping vlan <*vlan-id*> query-interval**	Configure this query interval. The "no **ip igmp snooping vlan <*vlan-id*> query-interval"** command restores the default value.
ip igmp snooping vlan <*vlan-id*> immediately-leave **no ip igmp snooping vlan <*vlan-id*> immediately-leave**	Enable the IGMP fast leave function for the specified VLAN: the "no **ip igmp snooping vlan <*vlan-id*> immediate-leave"** command disables the IGMP fast leave function.
ip igmp snooping vlan <*vlan-id*> query-mrsp <*value*> **no ip igmp snooping vlan <*vlan-id*> query-mrsp**	Configure the maximum query response period. The "no **ip igmp snooping vlan <*vlan-id*> query-mrsp"** command restores to the default value.
ip igmp snooping vlan <*vlan-id*> query-robustness <*value*> **no ip igmp snooping vlan <*vlan-id*> query-robustness**	Configure the query robustness. The "no **ip igmp snooping vlan <*vlan-id*> query-robustness"** command restores to the default value.
ip igmp snooping vlan <*vlan-id*> suppression-query-time <*value*> **no ip igmp snooping vlan <*vlan-id*> suppression-query-time**	Configure the suppression query time. The "no **ip igmp snooping vlan <*vlan-id*> suppression-query-time"** command restores to the default value.
ip igmp snooping vlan <*vlan-id*> static-group <*A.B.C.D*> [source <*A.B.C.D*>] interface [ethernet | port-channel] <*IFNAME*> **no ip igmp snooping vlan <*vlan-id*> static-group <*A.B.C.D*> [source <*A.B.C.D*>] interface [ethernet | port-channel] <*IFNAME*>**	Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration.

ip igmp snooping vlan <*vlan-id*> report source-address <*A.B.C.D*> **no ip igmp snooping vlan <*vlan-id*> report source-address**	Configure forwarding IGMP packet source address, The no operation cancels the packet source address.
ip igmp snooping vlan <*vlan-id*> specific-query-mrsp <value> **no ip igmp snooping vlan <*vlan-id*> specific-query-mrspt**	Configure the maximum query response time of the specific group or source, the no command restores the default value.

1.10.3 IGMP Snooping Examples

Scenario 1: IGMP Snooping function

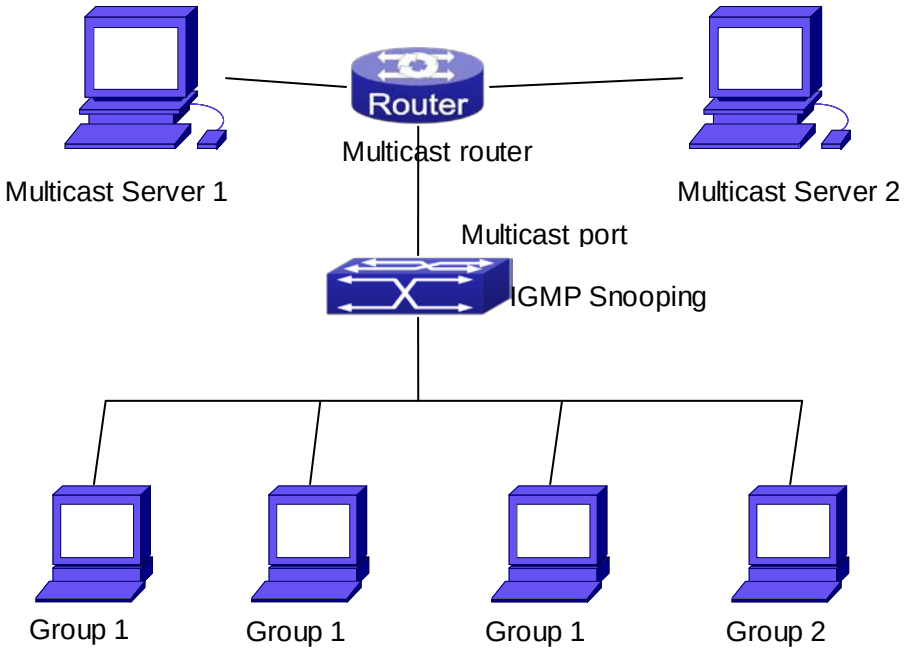


Fig 1-10 Enabling IGMP Snooping function

Example: As shown in the above figure, a VLAN 100 is configured in the switch and includes ports 1, 2, 6, 10 and 12. Four hosts are connected to port 2, 6, 10 and 12 respectively and the multicast router is connected to port 1. As IGMP Snooping is disabled by default either in the switch or in the VLANs, If IGMP Snooping should be enabled in VLAN 100, the IGMP Snooping should be first enabled for the switch in Global Mode and in VLAN 100 and set port 1 of VLAN 100 to be the mrouter port.

The configuration steps are listed below:

Switch(config)#ip igmp snooping

Switch(config)#ip igmp snooping vlan 100

Switch(config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/0/1

Multicast Configuration

Suppose two programs are provided in the Multicast Server using multicast address Group1 and Group2, three of four hosts running multicast applications are connected to port 2, 6, 10 plays program1, while the host is connected to port 12 plays program 2.

IGMP Snooping listening result:

The multicast table built by IGMP Snooping in VLAN 100 indicates ports 1, 2, 6, 10 in Group1 and ports 1, 12 in Group2.

All the four hosts can receive the program of their choice: ports 2, 6, 10 will not receive the traffic of program 2 and port 12 will not receive the traffic of program 1.

Scenario 2: L2-general-querier

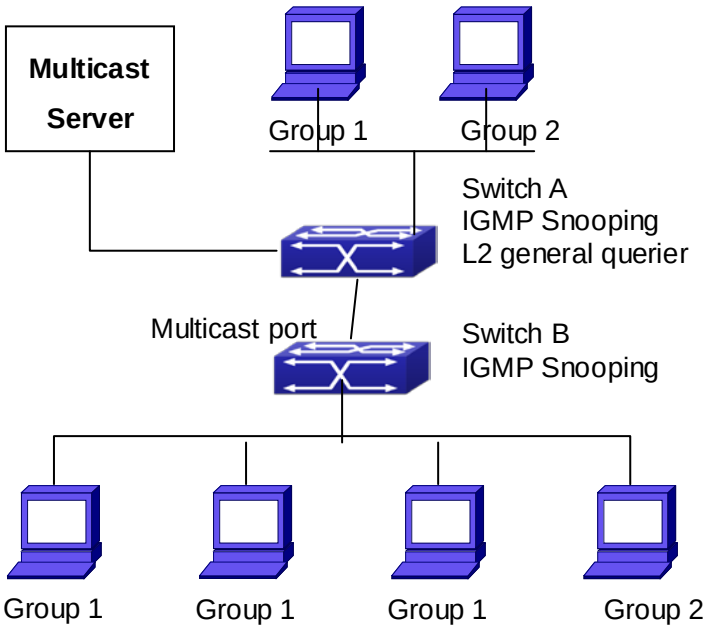


Fig 1-11 The switches as IGMP Queries

The configuration of Switch2 is the same as the switch in scenario 1, SwitchA takes the place of Multicast Router in scenario 1. Let's assume VLAN 60 is configured in SwitchA, including ports 1, 2, 10 and 12. Port 1 connects to the multicast server, and port 2 connects to Switch2. In order to send Query at regular interval, IGMP query must enabled in Global mode and in VLAN60.

The configuration steps are listed below:

SwitchA#config

SwitchA(config)#ip igmp snooping
SwitchA(config)#ip igmp snooping vlan 60
SwitchA(config)#ip igmp snooping vlan 60 L2-general-querier

SwitchB#config
SwitchB(config)#ip igmp snooping
SwitchB(config)#ip igmp snooping vlan 100
SwitchB(config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/0/1

Multicast Configuration
The same as scenario 1
IGMP Snooping listening result:
Similar to scenario 1

Scenario 3: To run in cooperation with layer 3 multicast protocols.
SWITCH which is used in Scenario 1 is replaced with ROUTER with specific configurations remains the same. And multicast and IGMP snooping configurations are the same with what it is in Scenario 1. To configure PIM-SM on ROUTER, and enable PIM-SM on vlan 100 (use the same PIM mode with the connected multicast router)

Configurations are listed as below:
switch#config
switch(config)#ip pim multicast-routing
switch(config)#interface vlan 100
switch(config-if-vlan100)#ip pim sparse-mode

IGMP snooping does not distribute entries when layer 3 multicast protocol is enabled. It only does the following tasks.

- ☞ Remove the layer 2 multicast entries.
- Provide query functions to the layer 3 with vlan, S, and G as the parameters.
- When layer 3 IGMP is disabled, re-enable distributing layer 2 multicast entries.

By looking up the layer 3 IPMC entries, it can be found that ports can be indicated by the layer 3 multicast entries. This ensures the IGMP snooping can work in cooperation with the layer 3 multicast protocols.

1.10.4 IGMP Snooping Troubleshooting

On IGMP Snooping function configuration and usage, IGMP Snooping might not run

properly because of physical connection or configuration mistakes. So the users should note that:

- ☞ Make sure correct physical connection
- ☞ Activate IGMP Snooping on whole configuration mode (use **ip igmp snooping**)
- ☞ Configure IGMP Snooping at VLAN on whole configuration mode (use **ip igmp snooping vlan <vlan-id>**)
- ☞ Make sure one VLAN is configured as L2 common checker in same mask, or make sure configured static mrouter
- ☞ Use **show ip igmp snooping vlan <vid>** command check IGMP Snooping information

1.11 IGMP Proxy Configuration

1.11.1 Introduction to IGMP Proxy

IGMP/MLD proxy which is introduced in rfc4605, is a simplified multicast protocol running at edge boxes. The edge boxes which runs the IGMP/MLD proxy protocol, does not need to run complicated multicast routing protocols such as PIM/DVMRP. However they work with multicast protocol enabled network through IGMP/MLD proxy. They can simplify the implementation of multicasting on edge devices.

The IGMP/MLD proxy works between the multicast router and the client, it works as both the multicast host and router. Upstream and downstream ports should be specified in the IGMP/MLD proxy configuration. The host protocol runs at upstream ports, while the router protocol runs at downstream ports. The switch collects the join and leave messages received from downstream ports and forward them to the multicast router through upstream ports.

The IGMP proxy configuration is exclusive with PIM and DVMRP configuration.

1.11.2 IGMP Proxy Configuration Task List

1. Enable IGMP Proxy function
2. Enable configurations for both downstream and upstream ports for the IGMP Proxy in different interfaces
3. Configure IGMP Proxy

1. Enable IGMP Proxy function

Command	Explanation
Global Mode	
ip igmp proxy **no ip igmp proxy**	Enable IGMP Proxy function. The "**no ip igmp proxy**" disables this function.

2. Enable configurations for both downstream and upstream ports for the IGMP Proxy in different interfaces

Command	Explanation
Interface Configuration Mode	
ip igmp proxy upstream **no ip igmp proxy upstream**	Enable IGMP Proxy upstream function. The "**no ip igmp proxy upstream**" disables this function.
ip igmp proxy downstream **no ip igmp proxy downstream**	Enable IGMP Proxy downstream function. The "**no ip igmp proxy downstream**" disables this function.

3. Configure IGMP Proxy assistant parameter

Command	Explanation
Global Mode	
ip igmp proxy limit {group *<1-500>*| source *<1-500>*} **no ip igmp proxy limit**	To configure the maximum number of groups that upstream ports can join, and the maximum number of sources in a single group. The no form of this command will restore the default value.
ip igmp proxy unsolicited-report interval *<1-5>* **no ip igmp proxy unsolicited-report interval**	To configure how often the upstream ports send out unsolicited report. The no form of this command will restore the default configuration.
ip igmp proxy unsolicited-report robustness *<2-10>* **no ip igmp proxy unsolicited-report robustness**	To configure the retry times of upstream ports' sending unsolicited reports. The no form of this command will restore the default value.
ip igmp proxy aggregate **no ip igmp proxy aggregate**	To configure non-query downstream ports to be able to aggregate the IGMP operations. The no form of this command will restore the default configuration.

ip multicast ssm range <*1-99*> **ip multicast ssm default** **no ip mulitcast ssm**	To configure the address range for IGMP proxy ssm multicast groups; The no form of this command will remove the configuration.
ip igmp proxy multicast-source **no ip igmp proxy multicast-source**	To configure the port as downstream ports for the source of multicast datagram; The no from of this command will disable the configuration.

1.11.3 IGMP Proxy Examples

Example 1: IGMP Proxy function.

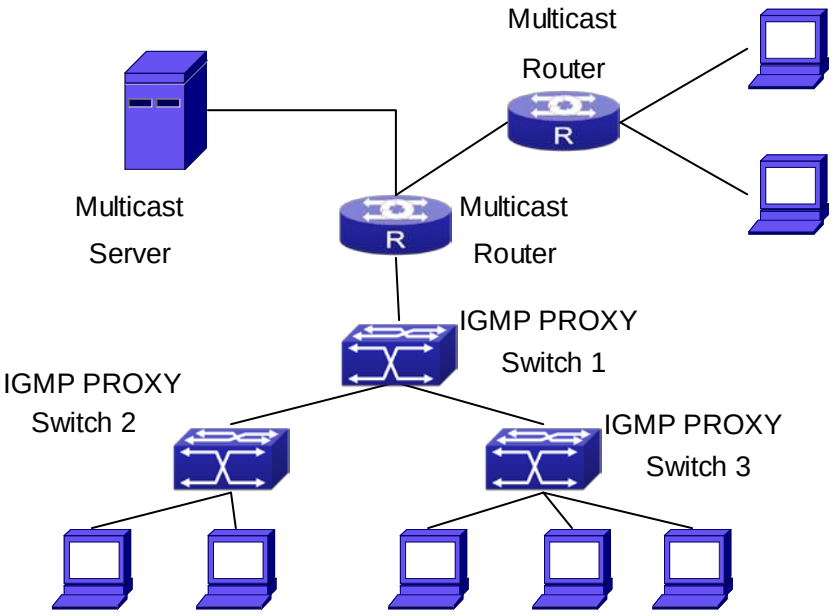


Fig 1-12 IGMP Proxy Topology Diagram

As it is show in the figure above, the switch functions as IGMP Proxy in a network of topology of tree, the switch aggregates the multicast dataflow from upstream port and redistributes them to the downstream ports, while the IGMP membership reports flow from downstream ports to upstream ports. Three IGMP Proxy enabled switches which are connected in tree topology, respectively have one port connected to multicast routers, and no less than one ports connected to hosts or upstream ports from other IGMP Proxy enabled switches.

The configuration steps are listed below:

Switch#config

Switch(config)#ip igmp proxy

Switch(Config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp proxy upstream

Switch(Config)#interface vlan 2

Switch(Config-if-Vlan2)#ip igmp proxy downstream

Multicast Configuration:

Suppose the multicast server offers some programs through 224.1.1.1. Some hosts subscribe that program at the edge of the network. The IGMP multicast members report themselves to the downstream ports of IGMP Proxy enabled Switch 2 and Switch 3. Switch 2 and Switch 3 then aggregate the group membership information and send them through the upstream ports. Switch 1 finally forward these membership information to the multicast router when receiving the group membership information through upstream ports, and deliver the multicast dataflow through downstream ports.

Example2: IGMP Proxy for multicast sources from downstream ports.

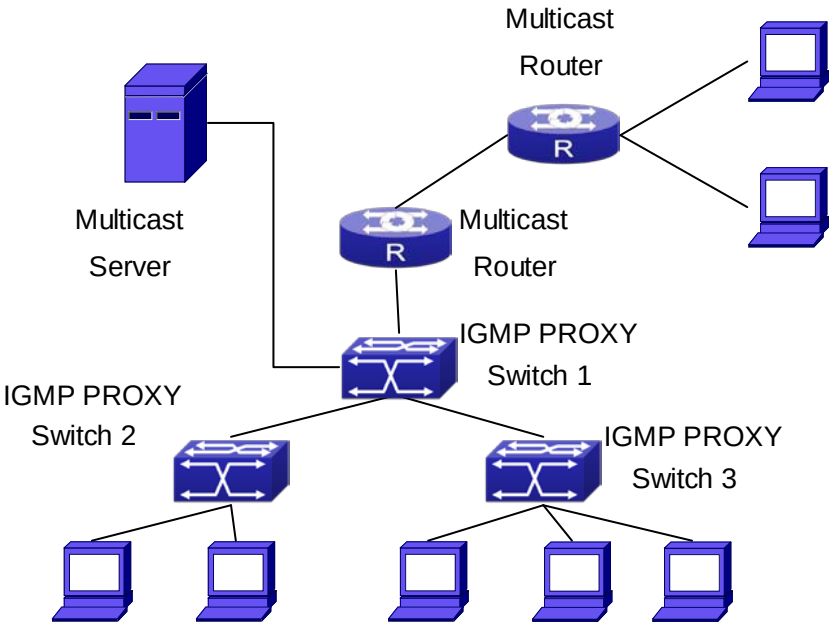


Fig 1-13 IGMP Proxy for multicast sources from downstream ports

As it is show in the figure above, IGMP Proxy enabled switches connected to the network in tree topology. The multicast source server connects to the downstream port of Switch1, the multicast dataflow is distributed through the upstream port and other

downstream ports. Three IGMP Proxy enabled switches which are connected in tree topology, respectively have one port connected to multicast routers, and no less than one ports connected to hosts or upstream ports from other IGMP proxy enabled switches.

The configuration steps are listed below:

IGMP PROXY Switch1 configuration:

Switch#config
Switch(config)#ip igmp proxy
Switch(Config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp proxy upstream
Switch(Config)#interface vlan 2
Switch(Config-if-Vlan2)#ip igmp proxy downstream
Switch(Config-if-Vlan2)#ip igmp proxy multicast-source

Route1 configuration:

Switch#config
Switch(config)#ip pim multicast
Switch(Config)#interface vlan 1
Switch(Config-if-Vlan1)#ip pim sparse-mode
Switch(Config-if-Vlan1)#ip pim bsr-border

Multicast Configuration:

Suppose the server provides programs through the multicast address 224.1.1.1, and some hosts subscribe that program on the edge of the network. The host reports their IGMP multicast group membership to Switch 2 and Switch 3 through downstream ports. Switch 2 and Switch 3 then aggregate and forward them to Switch 1 which then forwards the information to multicast router. When multicast dataflow arrives, the IGMP Proxy enabled switches re-distribute the group membership through upstream ports and downstream ports. When the multicast router receives the multicast dataflow from IGMP proxy, it will consider the multicast data source is directly connected to the router, and determine the identity of DR and ORIGINATOR. The multicast dataflow will be redistributed according to the PIM protocol.

1.11.4 IGMP Proxy Troubleshooting

When IGMP Proxy function configuration and usage, IGMP Proxy might not run properly because of physical connection or configuration mistakes. So the users should note that:

- ☞ Make sure physical connection correctly;
- ☞ Activate IGMP Proxy on whole Global mode (use **ip igmp proxy**);

- ☞ Make sure configure one upstream port and at least one downstream port under interface configuration mode (Use **ip igmp proxy upstream**, **ip igmp proxy downstream**);
- ☞ Use **show ip igmp proxy** command to check if the IGMP Proxy information is correct.

If the IGMP Proxy problem remains unsolved, please use debug IGMP Proxy and other debugging command and copy the DEBUG message within three minutes, send the recorded message to the technical service center of our company.

Chapter 2 IPv6 Multicast Protocol

2.1 PIM-DM6

2.1.1 Introduction to PIM-DM6

PIM-DM6（Protocol Independent Multicast, Dense Mode）is the IPv6 version of Protocol Independent Multicast Dense Mode. It is a Multicast Routing Protocol in dense mode which adapted to small network. The members of multicast group are relatively dense under this kind of network environment. There is no difference compared with the IPv4 version PIM-DM except that the addresses it uses are IPv6 addresses. Thus we don't differentiate between PIM-DM and PIM-DM6 in this chapter. All PIM-DM in the text without specific explanation refers to IPv6 version PIM-DM.

As a result of continuous development of IPv6 network, it has the network environment of nonsupport IPv6 multicast sometimes, so it needs to do the IPv6 multicast operation by tunnel. Therefore, our PIM-DM6 supports configuration on configure tunnel, and passes through nonsupport IPv6 multicast network by single cast packet of IPv4 encapsulation.

The working process of PIM-DM can be summarized as: Neighbor Discovery, Flooding-Prune, and Graft.

1. Neigh hour Discovery

When PIM-DM router is started at beginning, Hello message is required to discover neighbors. The network nodes running PIM-DM use Hello message to contact each other. PIM-DM Hello message is sent periodically.

2. Flooding-Prune

PIM-DM assumes that all hosts on the network are ready to receive multicast data. When certain multicast source S begins to send data to a multicast group G, after receiving the multicast packet, the router will make RPF examination first according to the unicast table. If the check passes, the router will create a (S, G) table item and forward the multicast packet to all downstream PIM-DM nodes (Flooding). If the RPF examination fails, i.e. the multicast packet is inputted from the incorrect interface, and then the message is discarded. After this procedure, every node will create an (S, G) item in the PIM-DM multicast domain. If there is no multicast group member in the downstream nodes, then a Prune message is sent to upstream nodes notifying not to forward data to this multicast group any more. After receiving Prune message, the corresponding interfaces will be deleted from the output interface list corresponding with the multicast-forwarding item (S,

G). Through this process, a SPT (Shortest Path Tree) is established with source S as root. Prune process is started by a sub-router.

The process above is called Flooding-Prune process. Each pruned node also provides overtime mechanism at the same time. In case of overtime of prune, the router will restart flooding-prune process. Flooding-prune of PIM-DM is conducted periodically

3. RPF examination

Adopting RPF examination, PIM-DM establishes a multicast forwarding tree initiating from data source, using existing unicast routing table. When a multicast packet arrives, the router will determine the correctness of its coming path first. If the arrival interface is the interface connected to multicast source indicated by unicast routing, then this multicast packet is considered to be from the correct path; otherwise the multicast packet will be discarded as redundant message. The unicast routing message used as path judgment can root in any Unicast Routing Protocol, such as messages found by RIP, OSPF, etc. It doesn't rely on any specific unicast routing protocol.

4. Assert Mechanism

If two multicast router A and B in the same LAN segment have their own receiving paths to multicast source S, they will respectively forward multicast data packet to LAN after receiving the packet from multicast source S. Then downstream nodes multicast router C will receive two multicast packets that are exactly the same. Once router detects such circumstance, a unique forwarder will be selected through "assert" mechanism. The optimized forwarding path is selected through "assert" packet. If the priority and costs of two or more than two paths are same, the node with a larger IP address will be selected as the upstream neighbor of item (S, G), which will be responsible for forwarding the (S, G) multicast packet.

5. Graft

When the pruned downstream node needs to recover to forwarding status, this node uses Graft Message to notify upstream nodes to resume multicast data forwarding.

2.1.2 PIM-DM6 Configuration Task List

1. Enable PIM-DM (Required)
2. Configure static multicast routing entries (Optional)
3. Configure additional PIM-DM parameters (Optional)
   (1) Configure parameters for PIM-DM interfaces
      1) Configure the interval for PIM-DM hello messages
      2) Configure the interval for PIM-DM state-refresh messages
      3) Configure the boundary interfaces
      4) Configure the management boundary

4. Disable PIM-DM protocol

1. Enable the PIM-DM protocol

On the switch, PIM-DM can be enabled through two steps. Firstly PIM multicast routing should be enabled in global configuration mode, then PIM-DM should be configured for the specific interfaces.

Command	Explanation
Command configuration mode	
ipv6 pim multicast-routing	To enable PIM-DM multicast routing global. However, in order to enable PIM-DM for specific interfaces, the following command must be issued.

Enable PIM-SM for the specific interface:

Command	Explanation
Interface configuration mode	
ipv6 pim dense-mode	To enable PIM-DM for the specified interface (required).

2. Configure static multicast routing entries

Command	Explanation
Global configuration mode	
ipv6 mroute <*X:X::X:X*> <*X:X::X:X*> <*ifname*> <*.ifname*> **no ipv6 mroute <*X:X::X:X*> <*X:X::X:X*> [<*ifname*> <*.ifname*>]**	To configure IPv6 static multicast routing entries. The no form of this command will remove the specified routing entry.

3. Configure additional PIM-DM parameters

（**1**）Configure parameters for PIM-DM interfaces

1) Configure the interval for PIM-DM hello messages

Command	Explanation
Interface Configuration Mode	
ipv6 pim hello-interval <*interval*> **no ipv6 pim hello-interval**	To configure the interval for PIM-DM hello messages. The no form of this command will restore the default value.

2) Configure the interval for PIM-DM state-refresh messages

Command	Explanation
Interface Configuration Mode	

ipv6 pim state-refresh origination-interval **no ipv6 pim state-refresh origination-interval**	To configure the interval for sending PIM-DM state-refresh packets. The no form of this command will restore the default value.

3) Configure the boundary interfaces

Command	Explanation
Interface Configuration Mode	
ipv6 pim bsr-border **no ipv6 pim bsr-border**	To configure the interface as the boundary of PIM-DM6 protocol. On the boundary interface, STATE REFRESH messages will not be sent or received. The network connected the interface is considered as directly connected network. The no form of this command will remove the configuration.

4) Configure the management boundary

Command	Explanation
Interface Configuration Mode	
ipv6 pim scope-border *<500-599>*|*<acl_name>* **no ipv6 pim scope-border**	To configure PIM-DM6 management boundary for the interface and apply ACL for the management boundary. With default settings, ffx0::/13 is considered as the scope of the management group. If ACL is configured, then the scope specified by ACL permit command is the scope of the management group. acl_name should be standard IPv6 ACL name. The no form of this command will remove the configuration.

4. Disable PIM-DM protocol

Command	Notes
Interface Configuration Mode	
no ipv6 pim dense-mode	To disable PIM-DM for the specified interface.
Global Configuration Mode	
no ipv6 pim multicast-routing	To disable PIM-DM globally.

2.1.3 PIM-DM6 Typical Application

As shown in the following figure, add the Ethernet interfaces of Switch A and Switch B to

corresponding vlan, and start PIM-DM Protocol on each vlan interface.

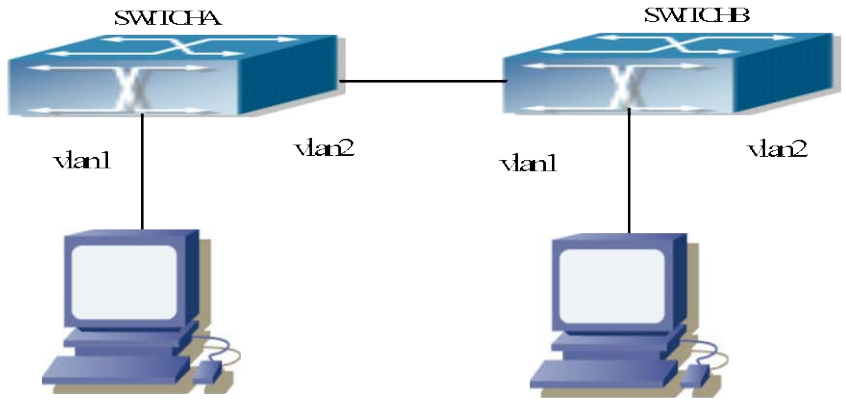


Fig 2-1 PIM-DM Typical Environment

The configuration procedure for SwitchA and SwitchB is as below:

(1) Configure SwitchA:

Switch(config)#ipv6 pim multicast-routing

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 address 2000:10:1:1::1/64

Switch(Config-if-Vlan1)#ipv6 pim dense-mode

Switch(Config-if-Vlan1)#exit

Switch(config)#interface vlan2

Switch(Config-if-Vlan2)#ipv6 address 2000:12:1:1:: 1/64

Switch(Config-if-Vlan2)#ipv6 pim dense-mode

(2) Configure SwitchB:

Switch(config)#ip pim multicast-routing

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 address 2000:12:1:1::2/64

Switch(Config-if-Vlan1)#ipv6 pim dense-mode

Switch(Config-if-Vlan1)#exit

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)#ipv6 address 2000:20:1:1::1/64

Switch(Config-if-Vlan2)#ipv6 pim dense-mode

2.1.4 PIM-DM6 Troubleshooting

When configuring and using PIM-DM protocol, PIM-DM protocol may fail to work normally due to physical connections, incorrect configuration and so on. So, users shall note the following points:

☞ Assure the physical connection is correct.

- ☞ Assure the Protocol of Interface and Link is UP (use show interface command);
- ☞ Assure PIM Protocol is turned on in Global Mode (use ipv6 pim multicast-routing command)
- ☞ Start PIM-DM Protocol on the interface (use ipv6 pim dense-mode command)

Unicast route shall be used to carry out RPF examination for multicast protocol. So the correctness of unicast route shall be guaranteed above all. If all attempts fail to solve the problems on PIM-DM, then use debug commands such as debug ipv6 pim, copy DEBUG information in 3 minutes and send to Technology Service Center.

2.2 PIM-SM6

2.2.1 Introduction to PIM-SM6

PIM-SM6（Protocol Independent Multicast, Sparse Mode）is the IPv6 version of Protocol Independent Multicast Sparse Mode. It is a multicast routing protocol in sparse mode and mainly used in large network with group members distributed relatively sparse and wide. It is no difference from the IPv4 version PIM-SM except the addresses it uses are IPv6 addresses. Thus we don't differentiate between PIM-SM and PIM-SM6 in this chapter. All PIM-SM in the text without specific explanation is IPv6 version PIM-SM. Unlike the Flooding-Prune of Dense Mode, PIM-SM Protocol assumes no host needs receiving multicast data packets. PIM-SM router forwards multicast data packets to a host only on definite request.

By setting RP (Rendezvous Point) and BSR (Bootstrap Router), PIM-SM announce multicast packet to all PIM-SM routers and establish, using Join/Prune message of routers, RPT (RP-rooted shared tree) based on RP. Consequently the network bandwidth occupied by data packets and control messages is cut down and the transaction cost of routers is reduced. Multicast data get to the network segment where the multicast group members are located along the shared tree flow. When the data traffic reaches a certain amount, multicast data stream can be switched to source-based SPT (Shortest Path Tree) to shorten network delay. PIM-SM doesn't rely on any specific unicast routing protocol but make RPF examination using existing unicast routing table.

1. PIM-SM Working Principle

The working process of PIM-SM mainly includes neighbor discovery, creation of RPT, registration of multicast source, SPT switch and so on. The neighbor discovery mechanism is the same with the mechanism of PIM-DM. We won't introduce any more.

(1) Creation of RP Shared Tree (RPT)

When a host joins a multicast group G, the leaf router directly connected with the

host finds out through IGMP message that there is a receiver of multicast group G, then it works out the corresponding Rendezvous Point RP for multicast group G, and send join message to upper level nodes in RP direction. Every router on the way from the leaf router to RP will create a (*, G) table item, indicating the message from any source to multicast group G is suitable for this item. When RP receives the message sent to multicast group G, the message will get to the leaf router along the established path and then reach the host. In this way, the RPT with RP as root is created.

(2) Multicast Source Registration

When multicast source S sends a multicast packet to multicast group G, the PIM-SM multicast router directly connected to it will take charge of sealing the multicast packet into registered message and unicast it to corresponding RP. If there are more than one PIM-SM multicast routers on a network segment, then DR (Designated Router) takes charge of forwarding the multicast packet.

(3) SPT Switch

Once the multicast router finds that the rate of the multicast packet from RP with destination address G exceeds threshold, the multicast router will send Join message to the upper lever nodes in the source direction, which results in the switch from RPT to SPT.

2. Preparation before PIM-SM configuration

(1) Configuration Candidate RP

More than one RPs (candidate RP) are permitted in PIM-SM network and each C-RP (Candidate RP) takes charge of forwarding multicast packets with destination address in a certain range. To configure more than one candidate RPs can achieve RP load balancing. There is no master or slave difference among RPs. All multicast routers work out the RP corresponded with certain multicast group based on the same algorithm after receiving the candidate RP message announced by BSR.

Note that one RP can serve more than one multicast groups, even all multicast groups. But each multicast group can only correspond with one unique RP at any moment. It can't correspond with more RPs at the same time.

(2) BSR Configuration

As the management core of PIMSM network, BSR is in charge of collecting messages sent by candidate RPs and broadcast them..

There may be only one BSR within a network. However, there may be several candidate BSRs to be configured. With such arrangement, once a BSR fails, another may be switched to. C-BSR determines BSR through automatic selection.

2.2.2 PIM-SM6 Configuration Task List

1. Enable PIM-SM (Required)

2. Configure static multicast routing entries (Optional)
3. Configure additional parameters for PIM-SM (Optional)

(1) Configure parameters for PIM-SM interfaces
   1) Configure the interval for PIM-SM hello messages
   2) Configure the holdtime for PIM-SM hello messages
   3) Configure ACL for PIM-SM6 neighbors
   4) Configure the interface as the boundary interface of the PIM-SM6 protocol
   5) Configure the interface as the management boundary of the PIM-SM6 protocol

(2) Configure global PIM-SM parameters
   1) Configure the switch as a candidate BSR
   2) Configure the switch as a candidate RP
      5) Configure static RP
   3) Configure the cache time of kernel multicast route

4. Disable the PIM-SM protocol

1. Enable PIM-SM protocol

The PIM-SM protocol can be enabled on Layer 3 switches by enabling PIM6 in global configuration mode and then enabling PIM-SM for specific interfaces in the interface configuration mode.

Command	Explanation
Global Configuration Mode	
[no] ipv6 pim multicast-routing	To enable the PIM-SM6 protocol for all the interfaces (However, in order to make PIM-SM work for specific interfaces, the following command should be issued). (required)

Make the PIM-SM protocol work for specific interfaces

Command	Explanation
Interface Configuration Mode	
[no] ipv6 pim sparse-mode [passive]	To enable PIM-SM for the specified interface. The no form of this command will disable the PIM-SM protocol (required).

2. Configure static multicast routing entries

Command	Explanation
Global Configuration Mode	

ipv6 mroute <*X:X::X:X*> <*X:X::X:X*> <*ifname*> <*.ifname*> **no ipv6 mroute <*X:X::X:X*> <*X:X::X:X*> [<*ifname*> <*.ifname*>]**	To configure a static multicast routing entry. The no form of this command will remove the specified static multicast routing entry.

3. Configure the additional parameters for PIM-SM

（1）Configure parameters for PIM-SM interfaces

1) Configure the interval for PIM-SM hello messages

Command	Explanation
Interface Configuration Mode	
ipv6 pim hello-interval <*interval*> **no ipv6 pim hello-interval**	To configure the interval for PIM-SM hello messages. The no form of this command restores the interval to the default value.

2) Configure the hold time for PIM-SM6 hello messages

Command	Explanation
Interface Configuration Mode	
ipv6 pim hello-holdtime <*value*> **no ipv6 pim hello-holdtime**	To configure the value of the holdtime field in the PIM-SM hello messages. The no form of this command will restore the hold time to the default value.

3) Configure ACL for PIM-SM6 neighbors

Command	Explanation
Interface Configuration Mode	
ipv6 pim neighbor-filter <*acess-list-name*> **no ipv6 pim neighbor-filter <*acess-list-name*>**	To configure ACL to filter PIM-SM6 neighbor. If session to the neighbor has been denied by ACL, then the sessions that have been set up will be discarded immediately and new sessions will not be set up.

4) Configure the interface as the boundary interface of the PIM-SM6 protocol

Command	Explanation
Interface Configuration Mode	
ipv6 pim bsr-border **no ipv6 pim bsr-border**	To configure the interface as the boundary of PIM-SM6 protocol. On the boundary interface, BSR messages will not be sent or received. The network connected the interface is considered as directly connected network. The no form of this command will remove the configuration.

5) Configure the interface as the management boundary of the PIM-SM6 protocol

Command	Explanation
Interface Configuration Mode	
ipv6 pim scope-border <*500-599*>|<*acl_name*> **no ipv6 pim scope-border**	To configure PIM-SM6 management boundary for the interface and apply ACL for the management boundary. With default settings, ffx0::/13 is considered as the scope of the management group. If ACL is configured, then the scope specified by ACL permit command is the scope of the management group. acl_name should be standard IPv6 ACL name. The no form of this command will remove the configuration.

（2）Configure global PIM-SM6 parameter

1) Configure the switch as a candidate BSR

Command	Explanation
Global Configuration Mode	
**ipv6 pim bsr-candiate {vlan <*vlan_id*>|<*ifname*>	tunnel <*1-50*>}[hash-mask-length] [priority]** **no Ipv6 pim bsr-candiate {vlan <*vlan_id*>|<*ifname*>	tunnel <*1-50*>}[hash-mask-length] [priority]**	This command is the global candidate BSR configuration command, which is used to configure the information of PIM-SM candidate BSR so that it can compete for BSR router with other candidate BSR. The no operation is to cancel the configuration of BSR.

2) Configure the switch as a candidate RP

Command	Explanation
Global Configuration Mode	
ipv6 pim rp-candiate {vlan<*vlan-id*>| loopback<*index*>|<*ifname*>} [<*group range*>] [<*priority*>] **no ipv6 pim rp-candiate**	This command is the global candidate RP configuration command, which is used to configure the information of PIM-SM candidate RP so that it can compete for RP router with other candidate RP. The no operation is to cancel the configuration of RP.

3) Configure static RP

Command	Explanation
Global Configuration Mode	

ipv6 pim rp-address <*rp-address*> [<*group-range*>] **no ipv6 pim rp-address <*rp-address*> {all|<*group-range*>}**	To configure the address of the candidate RP. The no form of this command will remove the configuration for the candidate RP.

4) Configure the cache time of kernel multicast route

Command	Explanation
Global Configuration Mode	
ipv6 multicast unresolved-cache aging-time <value> **no ipv6 multicast unresolved-cache aging-time**	Configure the cache time of kernel multicast route, the no command restores the default value.

4. Disable PIM-SM protocol

Command	Explanation
Interface Configuration Mode	
no ipv6 pim sparse-mode	To disable the PIM-SM6 protocol.
Global Configuration Mode	
no ipv6 pim sparse-mode	To disable PIM-DM globally.

2.2.3 PIM-SM6 Typical Application

As shown in the following figure, add the Ethernet interfaces of SwitchA, SwitchB, SwitchC and SwitchD to corresponding VLAN, and start PIM-SM Protocol on each VLAN interface.

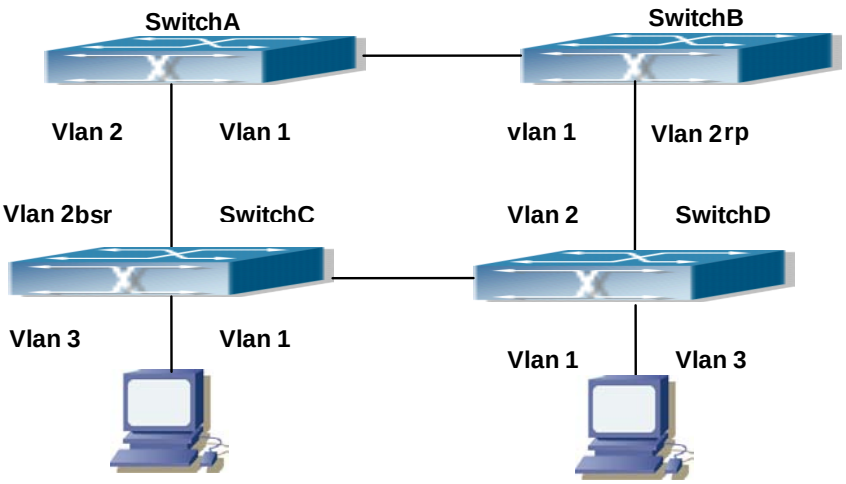


Fig 2-2 PIM-SM Typical Environment

The configuration procedure for SwitchA, SwitchB, SwitchC and SwitchD is as below:

(1) Configure SwitchA:

```
Switch(config)#ipv6 pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 address 2000:12:1:1::1/64
Switch(Config-if-Vlan1)#ipv6 pim sparse-mode
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 address 2000:13:1:1::1/64
Switch(Config-if-Vlan2)#ipv6 pim sparse-mode
```

(2) Configure Switch B:

```
Switch(config)#ipv6 pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 address 2000:12:1:1::2/64
Switch(Config-if-Vlan1)#ipv6 pim sparse-mode
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 address2000:24:1:1::2/64
Switch(Config-if-Vlan2)#ipv6 pim sparse-mode
Switch(Config-if-Vlan2)#exit
Switch(config)#ipv6 pim rp-candidate vlan2
```

(3) Configure SwitchC:

```
Switch(config)#ipv6 pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 address 2000:34:1:1::3/64
Switch(Config-if-Vlan1)#ipv6 pim sparse-mode
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 address 2000:13:1:1::3/64
Switch(Config-if-Vlan2)#ipv6 pim sparse-mode
Switch(Config-if-Vlan2)#exit
Switch(config)#interface vlan 3
Switch(Config-if-Vlan3)#ipv6 address 2000:30:1:1::1/64
Switch(Config-if-Vlan3)#ipv6 pim sparse-mode
Switch(Config-if-Vlan3)#exit
Switch(config)#ipv6 pim bsr-candidate vlan2 30 10
```

(4) Configure SwitchD:

```
Switch(config)#ipv6 pim multicast-routing
```

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 address 2000:34:1:1::4/64
Switch(Config-if-Vlan1)#ipv6 pim sparse-mode
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 address 2000:24:1:1::4/64
Switch(Config-if-Vlan2)#ipv6 pim sparse-mode
Switch(Config-if-Vlan2)#exit
Switch(config)#interface vlan 3
Switch(Config-if-Vlan3)#ipv6 address 2000:40:1:1::1/64
Switch(Config-if-Vlan3)#ipv6 pim sparse-mode
```

2.2.4 PIM-SM6 Troubleshooting

When configuring and using PIM-SM protocol, PIM-SM protocol may fail to work normally due to physical connections, incorrect configuration and so on. So, users shall note the following points:

- ☞ Assure the physical connection is correct.
- ☞ Assure the Protocol of Interface and Link is UP (use show interface command);
- ☞ Unicast route shall be used to carry out RPF examination for multicast protocol. So the correctness of unicast route shall be guaranteed above all.
- ☞ PIM-SM Protocol requires supports of RP and BSR, therefore you should use show ipv6 pim bsr-router first to see if there is BSR information. If not, you need to check if there is unicast routing leading to BSR.
- ☞ Use show ipv6 pim rp-hash command to check if RP information is correct; if there is no RP information, you still need to check unicast routing;

If all attempts fail to solve the problems on PIM-SM, then use debug commands such as debug ipv6 pim/ debug ipv6 pim bsr, copy DEBUG information in 3 minutes and send to Technology Service Center.

2.3 ANYCAST RP v6 Configuration

2.3.1 Introduction to ANYCAST RP v6

Anycast RP v6 is a technology based on PIM protocol, which provides redundancy in order to recover as soon as possible once an RP becomes unusable.

The kernel concept of Anycast RP v6 is that the RP addresses configured all over the

whole network exist on multiple multicast servers (the most common situation is that every device providing ANYCAST RP uses LOOPBACK interface, and using the longest mask to configures RP addresses on this interface), while the unicast routing algorithm will make sure that PIM routers can always find the nearest RP, thus , providing a shorter and faster way to find RP in a larger network., Once an RP being used becomes unusable, the unicast routing algorithm will ensure that the PIM router can find a new RP path fast enough to recover the multicast server in time. Multiple RP will cause a new problem that is if the multicast source and the receivers are registered to different RP, some receivers will not be able to receive data of multicast source (obviously, the register messages only prefer the nearest RP). So, in order to keep the communication between all RP, Anycast RP defines that the nearest RP to the multicast source should forward the source register messages to all the other RP to guarantee that all joiners of the RP can find the multicast source.

The method to realize the PIM-protocol-based Anycast RP is that: maintaining an ANYCAST RP list on every switch configured with Anycast RP and using another address as the label to identify each other. When one Anycast RP device receives a register message, it will send the register message to other Anycast RP devices while using its own address as the source address, to notify all the other devices of the original destination.

2.3.2 ANYCAST RP v6 Configuration Task

1. Enable ANYCAST RP v6 function
2. Configure ANYCAST RP v6

1. Enable ANYCAST RP v6 function

Command	Explanation
Global Configuration Mode	
ipv6 pim anycast-rp **no ipv6 pim anycast-rp**	Enable ANYCAST RP function. (necessary) The no operation will globally disable the ANYCAST RP function.

2. Configure ANYCAST RP v6

(1) Configure RP candidate

Command	Explanation
Global Configuration Mode	
ipv6 pim rp-candidate {vlan<*vlan-id*> |loopback<*index*> |<*ifname*>}	Now, the PIM-SM has allowed the Loopback interface to be a RP

[<*A:B::C:D*>][<*priority*>] **no ipv6 pim rp-candidate**	candidate.(necessary) Please pay attention to that, ANYCAST RP protocol can configure the Loopback interface or a regular three-layer VLAN interface to be the RP candidate. In make sure that PIM routers in the network can find where the RP locates, the RP candidate interface should be added into the router. No operation will cancel the RP candidate configured on this router.

(2) Configure self-rp-address (the RP communication address of this router)

Command	Explanation
Global Configuration Mode	
ipv6 pim anycast-rp self-rp-address A:B::C:D **no ipv6 pim anycast-rp self-rp-address**	Configure the self-rp-address of this router (as a RP). This address can be used to exclusively identify this router when communicating with other RP.(necessary) the effect of **self-rp-address** refers to two respects: 1 Once this router (as a RP) receives the register message from a DR unicast, it needs to forward the register message to all the other RP in the network, notifying them of the state of source (S.G). While forwarding the register message, this router will change the source address of it into self-rp-address. 2 Once this router(as a RP) receives a register message from other RP unicast, such as a register message whose destination is the self-rp-address of this router, it will create (S,G) state and send back a register-terminating message, whose destination address is the source address of the register message. Pay attention: self-rp-address has to be the

	address of a three-layer interface on this router, but the configuration is allowed to be done with the absence of the interface. The self-rp-address should be unique. No operation will cancel the self-rp-address which is used to communicate with other RP by this router.

(3) Configure other-rp-address (other RP communication addresses)

Command	Explanation
Global Configuration Mode	
ipv6 pim anycast-rp <*anycast-rp-addr*> <*other-rp-addr*> **no ipv6 pim anycast-rp <*anycast-rp-addr*> <*other-rp-addr*>**	Configure anycast-rp-addr on this router (as a RP). This unicast address is actually the RP address configured on multiple RP in the network, in accordance with the address of RP candidate interface (or Loopback interface). The effect of **anycast-rp-addr** includes: 1 Although more than one anycast-rp-addr addresses are allowed to be configured, only the one having the same address with the currently configured RP candidate address will take effect. Only after that, can the other-rp-address in accordance with this anycast-rp-addr take effect. 2 The configuration is allowed to be done with the absence of the interface in accordance with the anycast-rp-addr. Configure on this router (as a RP) the other-rp-addresses of other RP communicating with it. This unicast address identifies other RP and is used in the communication with local routers. The effect of **other-rp-address** refers to two respects: 1 Once this router (as a RP) receives the register message from a DR unicast, it should forward it to other RP in the network

	to notify all the RP in the network of the source (S.G) state. While forwarding, the router will change the destination address of the register message into other-rp-address. 2 Multiple other-rp-addresses can be configured in accordance with one anycast-rp-addr, Once the register message from a DR is received, it should be forwarded to all of this RP one by one. No operation will cancel other-rp-address communicating with this router.

2.3.3 ANYCAST RP v6 Configuration Examples

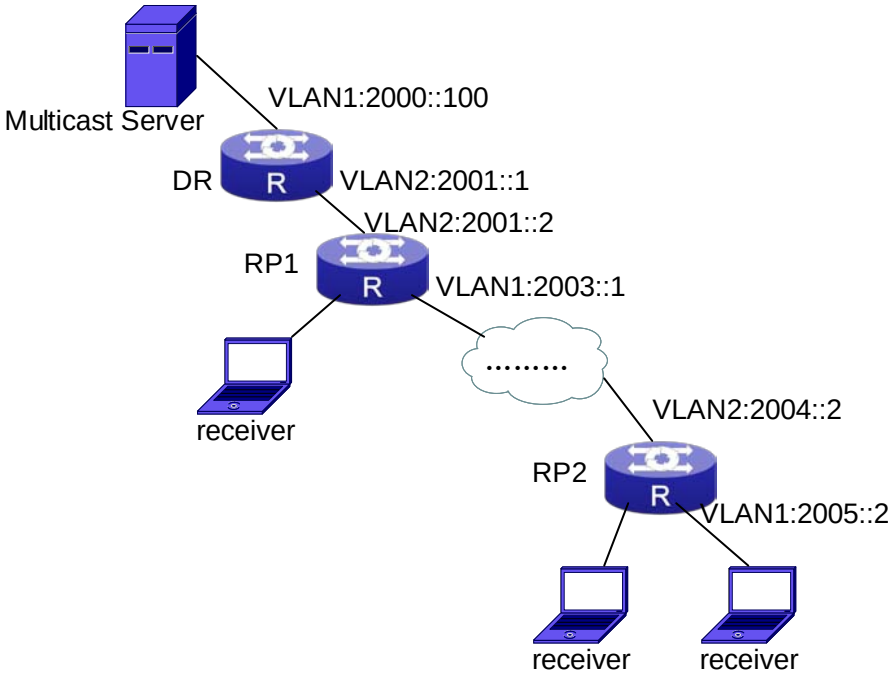


Fig 2-3 The ANYCAST RP v6 function of a router

The following is the configuration steps:

RP1 Configuration:

Switch#config

Switch(config)#interface loopback 1

Switch(Config-if-Loopback1)#ipv6 address 2006::1/128

Switch(Config-if-Loopback1)#exit

Switch(config)#ipv6 pim rp-candidate loopback1
Switch(config)#ipv6 pim bsr-candidate vlan 1
Switch(config)#ipv6 pim multicast-routing
Switch(config)#ipv6 pim anycast-rp
Switch(config)#ipv6 pim anycast-rp self-rp-address 2003::1
Switch(config)#ipv6 pim anycast-rp 2006::1 2004::2

RP2 Configuration:

Switch#config
Switch(config)#interface loopback 1
Switch(Config-if-Loopback1)#ipv6 address 2006::1/128
Switch(Config-if-Loopback1)#exit
Switch(config)#ipv6 pim rp-candidate loopback1
Switch(config)#ipv6 pim multicast-routing
Switch(config)#ipv6 pim anycast-rp
Switch(config)#ipv6 pim anycast-rp self-rp-address 2004::2
Switch(config)#ipv6 pim anycast-rp 2006::1 2003::1

Please pay attention to that, for promulgating loopback interface router, if use MBGP4+ protocol, then can use network command; or use RIPng protocol, then can use route command.

2.3.4 ANYCAST RP v6 Troubleshooting

When configuring and using ANYCAST RP v6 function, the ANYCAST RP might work abnormally because of faults in physical connections, configurations or something others. So, the users should pay attention to the following points:

- The physical connections should be guaranteed to be correct
- The PIM-SM6 protocol should be guaranteed to operate normally
- The ANYCAST RP should be guaranteed to be enabled in Global configuration mode
- The self-rp-address should be guaranteed to be configured correctly in Global configuration mode
- The other-rp-address should be guaranteed to be configured correctly in Global configuration mode
- All the interface routers should be guaranteed to be correctly added, including the loopback interface as a RP
- Use "**show ipv6 pim anycast rp status**" command to check whether the configuration information of ANYCAST RP is correct

If the problems of ANYCAST still cannot be solved after checking, please use debug commands like "debug ipv6 pim anycast-rp", then copy the DEBUG information within

three minutes and send it to the technical service center of our company.

2.4 PIM-SSM6

2.4.1 Introduction to PIM-SSM6

Source Specific Multicast (PIM-SSM6) is a new kind of multicast service protocol. With PIM-SSM6, a multicast session is distinguished by the multicast group address and multicast source address. In SSM6, hosts can be added into the multicast group manually and efficiently like the traditional PIM-SM6, but leave out the shared tree and RP management in PIM-S6M. In SSM6, SPT tree will be constructed with (S,G). G for the multicast group address and S for the source address of the multicast which sends datagram to G. (S,G) in a pair is named as a channel of SSM6. SSM6 serves best for the application of multicast service which is from one station to many ones, for example, the network sports video channel, and the news channel. By default, the multicast group address of SSM6 is limited to ff3x::/32. However this address range can be extended according to actual situations.

PIM-SSM6 can be supported in the PIM-DM6 environment.

2.4.2 PIM-SSM6 Configuration Task List

Command	Explanation
Global configuration mode	
ipv6 pim ssm {default|range <*access-list-number*>} **no ipv6 pim ssm**	To configure address range for pim-ssm multicast group. The no prefix will disable this command.

2.4.3 PIM-SSM6 Configuration Example

As it is shown in the below figure, ethernet interfaces of switchA, switchB, switchC, and switchD are separated into different vlan. And PIM-SM6 or PIM-DM6 is enabled on all the vlan interfaces. Take configuration of PIM-SM6 for example.

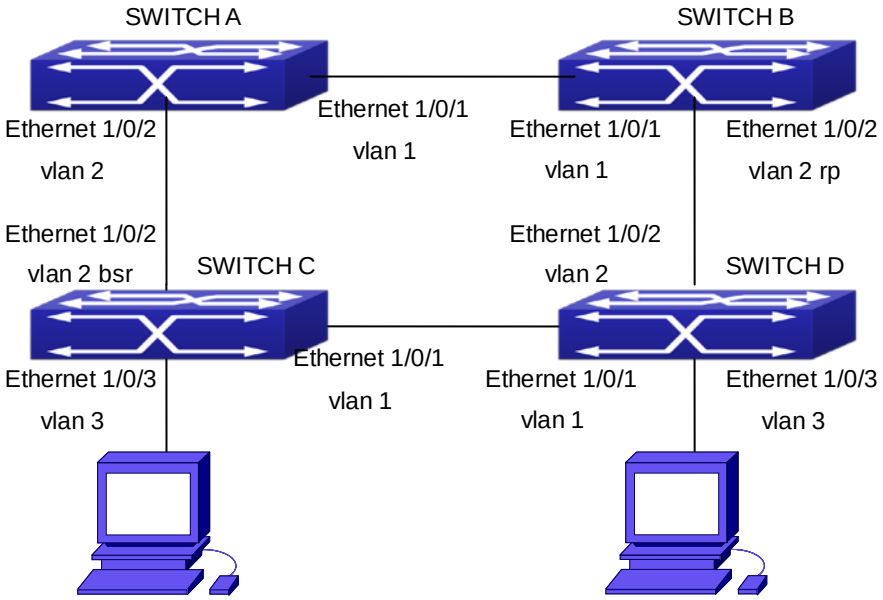


Fig 2-4 PIM-SSM typical environment

Configurations of switchA , switchB, switchC and switchD are listed as below:

(1) Configuration of switchA：

Switch(config)#ipv6 pim multicast-routing

Switch(config)#interface vlan 1

Switch(Config-If-Vlan1)# ipv6 address 2000:12:1:1::1/64

Switch(Config-If-Vlan1)# ipv6 pim sparse-mode

Switch(Config-If-Vlan1)#exit

Switch(config)#interface vlan 2

Switch(Config-If-Vlan2)# ipv6 address 2000:13:1:1::1/64

Switch(Config-If-Vlan2)# ipv6 pim sparse-mode

Switch(Config-If-Vlan2)#exit

Switch(config)#ipv6 access-list 500 permit ff1e::1/64

Switch(config)#ip pim ssm range 500

(2)Configuration of switchB：

Switch(config)#ipv6 pim multicast-routing

Switch(config)#interface vlan 1

Switch(Config-If-Vlan1)# ipv6 address 2000:12:1:1::2/64

Switch(Config-If-Vlan1)# ipv6 pim sparse-mode

Switch(Config-If-Vlan1)#exit

Switch(config)#interface vlan 2

Switch(Config-If-Vlan2)# ipv6 address2000:24:1:1::2/64

Switch(Config-If-Vlan2)# ipv6 pim sparse-mode

```
Switch(Config-If-Vlan2)# exit
Switch(config)# ipv6 pim rp-candidate vlan2
Switch(config)#ipv6 access-list 500 permit ff1e::1/64
Switch(config)#ip pim ssm range 500
```

(3) Configuration of SwitchC：

```
Switch(config)#ipv6 pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)# ipv6 address 2000:34:1:1::3/64
Switch(Config-If-Vlan1)# ipv6 pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-If-Vlan2)# ipv6 address 2000:13:1:1::3/64
Switch(Config-If-Vlan2)# ipv6 pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch(config)#interface vlan 3
Switch(Config-If-Vlan3)# ipv6 address 2000:30:1:1::1/64
Switch(Config-If-Vlan3)# ipv6 pim sparse-mode
Switch(Config-If-Vlan3)# exit
Switch(config)# ipv6 pim bsr-candidate vlan2 30 10
Switch(config)#ipv6 access-list 500 permit ff1e::1/64
Switch(config)#ip pim ssm range 500
```

(4) Configuration of SwitchD：

```
Switch(config)#ipv6 pim multicast-routing
Switch(config)#interface vlan 1
Switch(Config-If-Vlan1)# ipv6 address 2000:34:1:1::4/64
Switch(Config-If-Vlan1)# ipv6 pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-If-Vlan2)# ipv6 address 2000:24:1:1::4/64
Switch(Config-If-Vlan2)# ipv6 pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch(config)#interface vlan 3
Switch(Config-If-Vlan3)# ipv6 address 2000:40:1:1::1/64
Switch(Config-If-Vlan3)# ipv6 pim sparse-mode
Switch(Config-If-Vlan3)#exit
Switch(config)#ipv6 access-list 500 permit ff1e::1/64
```

Switch(config)#ip pim ssm range 500

2.4.4 PIM-SSM6 Troubleshooting

When configuring the PIM-SSM6 protocol, it may fail to work because of the failure of physical connection or the mis-configurations. To debug these errors, attention should be paid to the following lists.

- ☞ Make sure the physical links are connected correctly.
- ☞ Make sure the state of the data link layer has become UP. (Use show interface command).
- ☞ Make sure PIM6 is enabled in global configuration mode (Refer to the command ipv6 pim multicast-routing).
- ☞ Make sure PIM-SM6 is configured on the interface (Refer to the command ipv6 pim sparse-mode)
- ☞ Make sure SSM6 is configure in global configuration mode.
- ☞ The multicast protocol uses the unicast routing to make RPF check. Hence, single-cast routing should be verified firstly.

If problems could not be fixed with the above check list, please enable the command of **debug ipv6 pim event and debug ipv6 pim packet**, and save the debug information for 3 minutes, and send if to Technology Service Center.

2.5 IPv6 DCSCM

2.5.1 Introduction to IPv6 DCSCM

The technology of IPv6 DCSCM (Destination Control and Source Control Multicast) includes three aspects: the multicast source control, the multicast user control and the service-priority-oriented policy multicast.

IPv6 DCSCM Controllable Multicast technology proceeds as the following way:

1. If source controlled multicast is configured on the edge switches, only the multicast data of the specified group from the specified source can pass.
2. The RP switches which are the core of PIM-SM will directly send REGISTER_STOP as response to the REGISTER messages not from the specified source and specified group, and no entry is allowed to be created. (This task is implemented in the PIM-SM module).

The control of multicast users of IPv6 DCSCM technology is implemented on the basis of controlling the MLD message sent from the users, so the control module is MLD

snooping and the MLD module, the control logic of which includes the following three methods: controlling according to the VLAN+MAC sending the message, controlling according to the IP address sending the message, and controlling according to the input port of the message. MLD snooping can adopts all the three methods at the same time, while the MLD module, at the third layer, can only control the IP address sending the message.

The service-priority-oriented policy multicast of IPv6 DCSCM technology adopts the following method: for the confined multicast data, the user-specified priority will be set at the access point, enabling the data can be sent at a higher priority through TRUNK, and guaranteeing that the data can be sent through the whole net at the user-specified priority.

2.5.2 IPv6 DCSCM Configuration Task Sequence

1. The source control configuration
2. The destination control configuration
3. The multicast policy configuration

1. The source control configuration

The source control configuration has three steps, first is globally enabling the source control, the following is the command of globally enabling the source control:

Command	Explanation
Global Configuration Mode	
ipv6 multicast source-control(necessary) **no ipv6 multicast source-control**	Globally enable the source control, the no operation of this command will globally disable the source control. What should be paid attention to is that, once globally enable the source control, all the multicast messages will be dropped by default. All the source control configurations can only be done after globally enabled, and only when all the configured rules are disabled, the source control can be disabled globally.

The next is configuring the source control rules, which adopts the same method as configuring ACL, using ACL number from 8000 to 8099, while each rule number can configure 10 rules. What should be paid attention to is that these rules have orders, the earliest configured rule is at the front. Once a rule is matched, the following ones will not take effect, so the globally enabled rules should be the last to configure. The following is

the command:

Command	Explanation
Global Configuration Mode	
[no] ipv6 access-list <*8000-8099*> {deny|permit} {{<*source/M*>}|{host-source <*source-host-ip*>}|any-source} {{<*destination/M*> }|{host-destination <*destination-host-ip*>}|any-destination}	Used to configure the source control rules, the rules can only take effect when applied to the specified port. The no operation of this command can delete the specified rule.

The last is to configure the rules to the specified port.

Pay attention: since the configured rules will take up entries of hardware, configuring too many rules might cause failure if the underlying entries are full, so it is recommended that users adopt rules as simple as possible. The following is the configuration command:

Command	Explanation
Port Configuration Mode	
[no] ipv6 multicast source-control access-group <*8000-8099*>	Used to configure the source control rule to a port, he no operation will cancel this configuration.

2. The configuration of destination control

The configuration of destination control is similar to that of source control, and also has three steps:

First, globally enable the destination control, since destination control needs to avoid the unauthorized users from receiving multicast data, once it is enabled globally, the switch will stop broadcasting received multicast data, so if a switch has enabled destination control, users should not connect two or more other Layer three switches within the same VLAN where it locates. The following is the configuration command:

Command	Explanation
Global Configuration Mode	
multicast destination-control(necessary)	Globally enable IPV4 and IPv6 destination control, the no operation of this command will globally disable destination control. All of the other configuration can only take effect after globally enabled.

The next is configuring destination control rules, which are similar to that of source control, but using ACL number from 9000 to 10099 instead.

Command	Explanation
Global Configuration Mode	
[no] ipv6 access-list <*9000-10099*> {deny|permit} {{<*source/M*>}|{host-source <*source-host-ip*>}|any-source} {{<*destination/M*>}|{host-destination <*destination-host-ip*>}|any-destination}	Used to configure destination control rules, these rules can only take effect when applied to specified source IP, VLAN-MAC or port. The no operation of this rule will delete the specified rule.

The last step is to configure the rules to the specified source IP, source VLAN MAC or the specified port. What should be paid attention to is that only when the MLD-SNOOPING is enabled, these rules can be globally used, or, only rules of source IP can be used in MLD protocol. The following is the configuration command:

Command	Explanation
Port Mode	
[no] ipv6 multicast destination-control access-group <*9000-10099*>	Used to configure the destination control rule to a port, the no operation of this command will cancel the configuration.
Global Configuration Mode	
[no] ipv6 multicast destination-control <*1-4094*> <*macaddr*> access-group <*9000-10099*>	Used to configure the destination control rules to the specified VLAN-MAC, the no operation of this command will cancel the configuration.
[no] ipv6 multicast destination-control <*IPADDRESS/M*> access-group <*9000-100999*>	Used to configure the destination control rules to the specified source IPv6 address/MASK, the no operation of this command will cancel the configuration.

3. The configuration of multicast policy

The multicast policy adopts the method of specifying a priority for the specified multicast data to meet the user's particular demand, what should be paid attention to is that only when multicast data is transmitted in TRUNK, can it be taken special care of. The configuration is quite simple, for only one command is needed, that is set priority for the specified multicast, the following is the command:

Command	Explanation
Global Configuration Mode	

[no] ipv6 multicast policy <*IPADDRESS/M*> <*IPADDRESS/M*> cos <*priority*>	Configure multicast policy, set priority for sources and groups in a specified range, the priority valid range is 0 to 7.

2.5.3 IPv6 DCSCM Typical Examples

1. Source control

In order to prevent an edge switch sends multicast data at will, we configure on the edge switch that only the switch whose port is Ethernet1/0/4 can send multicast data, and the group of data should be ff1e::1. The uplink port Ethernet1/0/25 can forward multicast data without being restricted, so we can configure as follows.

Switch(config)#ipv6 access-list 8000 permit any-source ff1e::1

Switch(config)#ipv6 access-list 8001 permit any any

Switch(config)#ipv6 multicast source-control

Switch(config)#interface Ethernet1/0/4

Switch(Config-If-Ethernet1/0/4)#ipv6 multicast source-control access-group 8000

Switch(config)#interface Ethernet1/0/25

Switch(Config-If-Ethernet1/0/25)#ipv6 multicast source-control access-group 8001

2. Destination control

We want to confine that the users of the segment whose address is fe80::203:fff:fe01:228a/64 can not join the ff1e::1/64 group, so we can configure as follows:

First, enable MLD Snooping in the VLAN where it locates (in this example, it is VLAN2).

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping vlan 2

Then configure relative destination control access list and configure specified IPv6 address to use this access list.

Switch(config)#ipv6 access-list 9000 deny any ff1e::1/64

Switch(config)#ipv6 access-list 9000 permit any any

Switch(config)#multicast destination-control

Switch(config)#ipv6 multicast destination-control fe80::203:fff:fe01:228a/64 access-group 9000

Thus, the users of this segment can only join groups other than 2ff1e::1/64.

3. Multicast policy

Server 2008::1 is sending important multicast data in group ff1e::1, we can configure on its access switch as follows:

Switch(config)#ipv6 multicast policy 2008::1/128 ff1e::1/128 cos 4

Thus this multicast flow will have a priority of 4, when it passes the TRUNK port of this switch to another switch (generally speaking, it is a relatively high priority, the data with higher priority might be protocol data, if a higher priority is set, when there is too much multicast data, the switch protocol might operate abnormally).

2.5.4 IPv6 DCSCM Troubleshooting

IPv6 DCSCM module acts like ACL, so most problems are caused by improper configuration. Please read the instructions above carefully.

2.6 MLD

2.6.1 Introduction to MLD

MLD (Multicast Listener Discovery) is the multicast group member (receiver) discovery protocol serving IPv6 multicast. It is similar to IGMP Protocol in IPv4 multicast application. Correspondingly, MLD Protocol version1 is similar to IGMP Protocol version2, and MLD Protocol version2 is similar to IGMP Protocol version3. Current firmware supports MLDv1/ MLDv2.

The IPv6 multicast hosts can join or leave from multicast group at any location, any time, regardless of the total number of group members. It is unnecessary and impossible for multicast switch to store the relationship among all host members. Multicast switch simply finds out via MLD protocol if there are receivers of certain multicast group on the network segment connected to each port. The only thing host need to do is to keep the record of which multicast groups it joined.

MLD is unsymmetrical between host and switch: the host needs to respond the MLD query message of multicast switch with membership report message; the switch periodically sends membership query message and determines if there is host joining a specific group in its subnetworks according to the response message received, and after it receives the report of a host quitting from the group, it sends out the query for the group to confirm if there is no member left in it.

There are three types of protocol messages of MLD Protocol, that is, Query, Report and Done (which is corresponding to Leave of IGMPv2). Like IGMPV2, the Query messages include General Query and Specific Group Query. General Query uses the multicast address FF02::1 of hosts as destination address, the group address is 0; and Specific Group Query use its group address as destination address. The multicast

addresses of MLD use 130, 131 and 132 as data types denoting the three kinds of messages mentioned above. Other logic is basically same as IGMPv2.

MLD protocol version2 use FF02::16 as destination address of membership report, and 143 as data type. The other logic of MLD Protocol version2 is similar to IGMP Protocol version3.

2.6.2 MLD Configuration Task List

1、Start MLD (Required)

2、Configure MLD auxiliary parameters (Required)

（1）Configure MLD group parameters

1）Configure MLD group filter conditions

（2）Configure MLD query parameters

1）Configure the interval of MLD sending query message

2）Configure the maximum response time of MLD query

3）Configure overtime of MLD query

3、Shut down MLD Protocol

1. Start MLD Protocol

There is no special command for starting MLD Protocol on EDGECORE series layer 3 switches. MLD Protocol will automatically start up as long as any IPv6 multicast protocol is started on corresponding interface.

Command	Explanation
Global Mode	
Ipv6 pim multicast-routing	To start Global IPv6 Multicast Protocol, the precondition of starting MLD Protocol. The NO operation of corresponding command shuts ipv6 multicast protocol and MLD Protocol. (Required)

Command	**Explanation**
Port Configuration Mode	
ipv6 pim dense-mode | ipv6 pim sparse-mode	Start MLD Protocol. The NO operation of corresponding command shuts MLD Protocol. (Required)

2. Configure MLD auxiliary parameters

（1）Configure MLD group parameters

1）Configure MLD group filter conditions

Command	Explanation
Port Configuration Mode	
ipv6 mld access-group ***<acl_name>*** **no ipv6 mld access-group**	Configure the filter conditions of interface for MLD group; the NO operation of this command cancels filter conditions.

（2）Configure MLD Query parameters

1）Configure interval time for MLD to send query messages

2）Configure the maximum response time of MLD query

3）Configure the overtime of MLD query

Command	Explanation
Port Configuration Mode	
ipv6 mld query-interval ***<time_val>*** **no ipv6 mld query-interval**	Configure the interval of MLD query messages sent periodically; the NO operation of this command restores the default value.
ipv6 mld query-max-response-time ***<time_val>*** **no ipv6 mld query-max-response-time**	Configure the maximum response time of the interface for MLD query; the NO operation of this command restores the default value.
ipv6 mld query-timeout ***<time_val>*** **no ipv6 mld query-timeout**	Configure the overtime of the interface for MLD query; the NO operation of this command restores the default value.

3. Shut down MLD Protocol

Command	Explanation
Port Configuration Mode	
no ipv6 pim dense-mode | no ipv6 pim sparse-mode | no ipv6 pim multicast-routing (Global Mode)	Shut down MLD Protocol

2.6.3 MLD Typical Application

As shown in the following figure, add the Ethernet interfaces of Switch A and Switch B to corresponding vlan, and start PIM6 on each vlan interface.

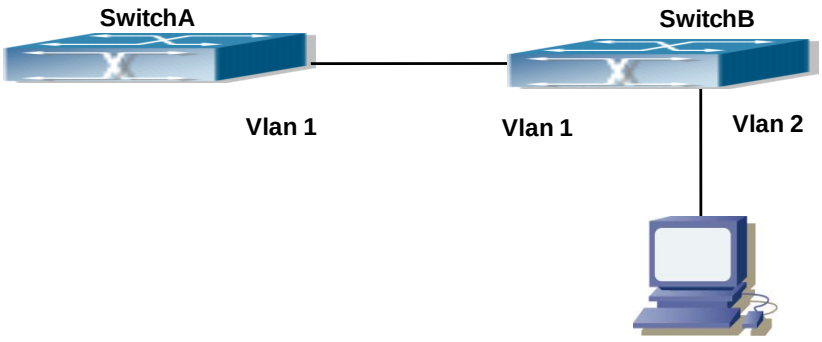


Fig 2-5 Network Topology Diagram

The configuration procedure for SwitchA and SwitchB is as below:

(1) Configure SwitchA:

Switch (config) #ipv6 pim multicast-routing

Switch (config) #ipv6 pim rp-address 3FFE::1

Switch (config) #interface vlan 1

Switch (Config-if-Vlan1) #ipv6 address 3FFE::1/64

Switch (Config-if-Vlan1) #ipv6 pim sparse-mode

(2) Configure SwitchB:

Switch (config) #ipv6 pim multicast-routing

Switch (config) #ipv6 pim rp-address 3FFE::1

Switch (config) #interface vlan1

Switch (Config-if-Vlan1) #ipv6 address 3FFE::2/64

Switch (Config-if-Vlan1) #ipv6 pim sparse-mode

Switch (Config-if-Vlan1) #exit

Switch (config) #interface vlan2

Switch (Config-if-Vlan2) #ipv6 address 3FFA::1/64

Switch (Config-if-Vlan2) #ipv6 pim sparse-mode

Switch (Config-if-Vlan2) #ipv6 mld query-timeout 150

2.6.4 MLD Troubleshooting Help

When configuring and using MLD protocol, MLD protocol may fail to work normally due to physical connections, incorrect configuration and so on. So, users shall note the following points:

- Assure the physical connection is correct.
- Assure the protocol of interface and link is UP (use show interface command)
- Assure to start one kind of multicast protocol on the interface
- Assure the time of the timers of each router on the same network segment is

consistent; usually we recommend the default setting.

☞ Unicast route shall be used to carry out RPF examination for multicast protocol. So the correctness of unicast route shall be guaranteed above all.

If all attempts fail to solve the problems on MLD, please use debug commands such as debug ipv6 MLD event/packet, and copy DEBUG information in 3 minutes and send to Technology Service Center.

2.7 MLD Snooping

2.7.1 Introduction to MLD Snooping

MLD, the Multicast Listener Discovery Protocol, is used to realize multicasting in the IPv6. MLD is used by the network equipments such as routers which supports multicast for multicast listener discovery, also used by listeners looking forward to join certain multicast group informing the router to receive data packets from certain multicast address, all of which are done through MLD message exchange. First the router send an MLD Multicast listener Query message through a multicast address which can address all the listeners (namely ff02::1). Once there is a listener who wishes to join the multicast address, it will send a MLD Multicast listener Report back through the multicast address.

MLD Snooping is namely the MLD listening. The switch restricts the multicast traffic from flooding through MLD Snooping, and forward the multicast traffic to ports associated to multicast devices only. The switch listens to the MLD messages between multicast routers and listeners, and maintains the multicast group forwarding list based on the listening result. The switches forwards multicast packets according to the multicast forwarding list

The switch realizes the MLD Snooping function while supporting MLD v2. This way, the user can acquire IPv6 multicast with the switch.

2.7.2 MLD Snooping Configuration Task

1. Enable the MLD Snooping function
2. Configure the MLD Snooping

1. Enable the MLD Snooping function

Command	Explanation
Global Mode	
ipv6 mld snooping **no ipv6 mld snooping**	Enable global MLD Snooping, the "**no ipv6 mld snooping**" command disables

	the global MLD snooping.

2. Configure MLD Snooping

Command	Explanation
Global Mode	
ipv6 mld snooping vlan <*vlan-id*> **no ipv6 mld snooping vlan <*vlan-id*>**	Enable MLD Snooping on specific VLAN. The “no” form of this command disables MLD Snooping on specific VLAN.
ipv6 mld snooping vlan <*vlan-id*> limit {group <*g_limit*> | source <*s_limit*>} **no ipv6 mld snooping vlan <*vlan-id*> limit**	Configure the number of the groups in which the MLD Snooping can join, and the maximum number of sources in each group. The “no” form of this command restores to the default.
ipv6 mld snooping vlan <*vlan-id*> l2-general-querier **no ipv6 mld snooping vlan <*vlan-id*> l2-general-querier**	Set the VLAN level 2 general querier, which is recommended on each segment. The “no” form of this command cancels the level 2 general querier configuration.
ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface <*interface –name*> **no ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface <*interface –name*>**	Configure the static mrouter port in specific vlan. The “no” form of this command cancels the mrouter port configuration.
ipv6 mld snooping vlan <*vlan-id*> mrouter-port learnpim6 **no ipv6 mld snooping vlan <*vlan-id*> mrouter-port learnpim6**	Enable the function that the specified VLAN learns mrouter-port (according to pimv6 packets), the no command will disable the function.
ipv6 mld snooping vlan <*vlan-id*> mrpt <*value*> **no ipv6 mld snooping vlan <*vlan-id*> mrpt**	Configure the keep-alive time of the mrouter port. The “no” form of this command restores to the default.
ipv6 mld snooping vlan <*vlan-id*> query-interval <*value*> **no ipv6 mld snooping vlan <*vlan-id*> query-interval**	Configure the query interval. The “no” form of this command restores to the default.
ipv6 mld snooping vlan <*vlan-id*> immediate-leave **no ipv6 mld snooping vlan <*vlan-id*> immediate-leave**	Configure immediate leave multicast group function for the MLD Snooping of specific VLAN. The “no” form of this command cancels the immediate leave configuration.
ipv6 mld snooping vlan <*vlan-id*> query-mrsp <*value*>	Configure the query maximum response period. The “no” form of this command

no ipv6 mld snooping vlan <*vlan-id*> query-mrsp	restores to the default.
ipv6 mld snooping vlan <*vlan-id*> query-robustness <*value*> **no ipv6 mld snooping vlan <*vlan-id*> query-robustness**	Configure the query robustness, the "no" form of this command restores to the default.
ipv6 mld snooping vlan <*vlan-id*> suppression-query-time <*value*> **no ipv6 mld snooping vlan <*vlan-id*> suppression-query-time**	Configure the suppression query time. The "no" form of this command restores to the default
Ipv6 mld snooping vlan <*vlan-id*> static-group <*X:X::X:X*> [source <*X:X::X:X*>] interface [ethernet | port-channel] <*IFNAME*> **no ipv6 mld snooping vlan <*vlan-id*> static-group <*X:X::X:X*> [source <*X:X::X:X*>] interface [ethernet | port-channel] <*IFNAME*>**	Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration.

2.7.3 MLD Snooping Examples

Scenario 1: MLD Snooping Function

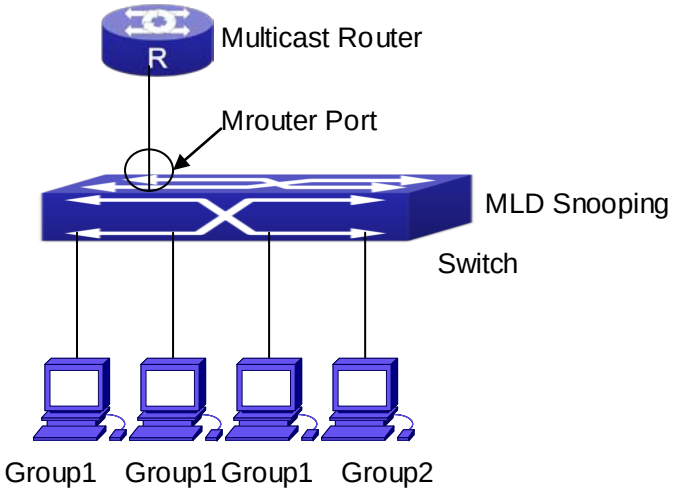


Fig 2-6 Open the switch MLD Snooping Function figure

As shown above, the vlan 100 configured on the switch consists of ports 1, 2, 6, 10 and 12. Four hosts are respectively connected to 2, 6, 10 and 12 while the multicast router on port 1. Suppose we need MLD Snooping on VLAN 100, however by default, the global MLD Snooping as well as the MLD Snooping on each VLAN are, therefore first we have to

enable the global MLD Snooping at the same time enable the MLD Snooping on VLAN 100, furthermore we need to set the port 1 of VLAN 100 as a mrouter port.

Configuration procedure is as follows.

Switch#config

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping vlan 100

Switch(config)#ipv6 mld snooping vlan 100 mrouter-port interface ethernet 1/0/1

Multicast configuration:

Assume there are two multicast servers: the Multicast Server 1 and the Multicast Server 2, amongst program 1 and 2 are supplied on the Multicast Server 1 while program 3 on the Multicast server 2, using group addresses respectively the Group 1, Group 2 and Group 3. Concurrently multicast application is operating on the four hosts. Two hosts connected to port 2, 6 are playing program 1 while the host connected to port 10 playing program 2, and the one to port 12 playing program 3.

MLD Snooping interception results:

The multicast table on vlan 100 shows: port 1, 2, 6 are in （Multicasting Server 1, Group1）, port1, 10 are in (Multicasting Server 1,Group2), and port1, 121, 12 are in (Multicasting Server 2, Group3）

All the four hosts successfully receive programs they are interested in. port2, 6 receives no traffic from program2 and 3; port10 receives no traffic from program 1 and 3, and port12 receives no traffic from program1 and 2.

Scenario 2: MLD L2-general-querier

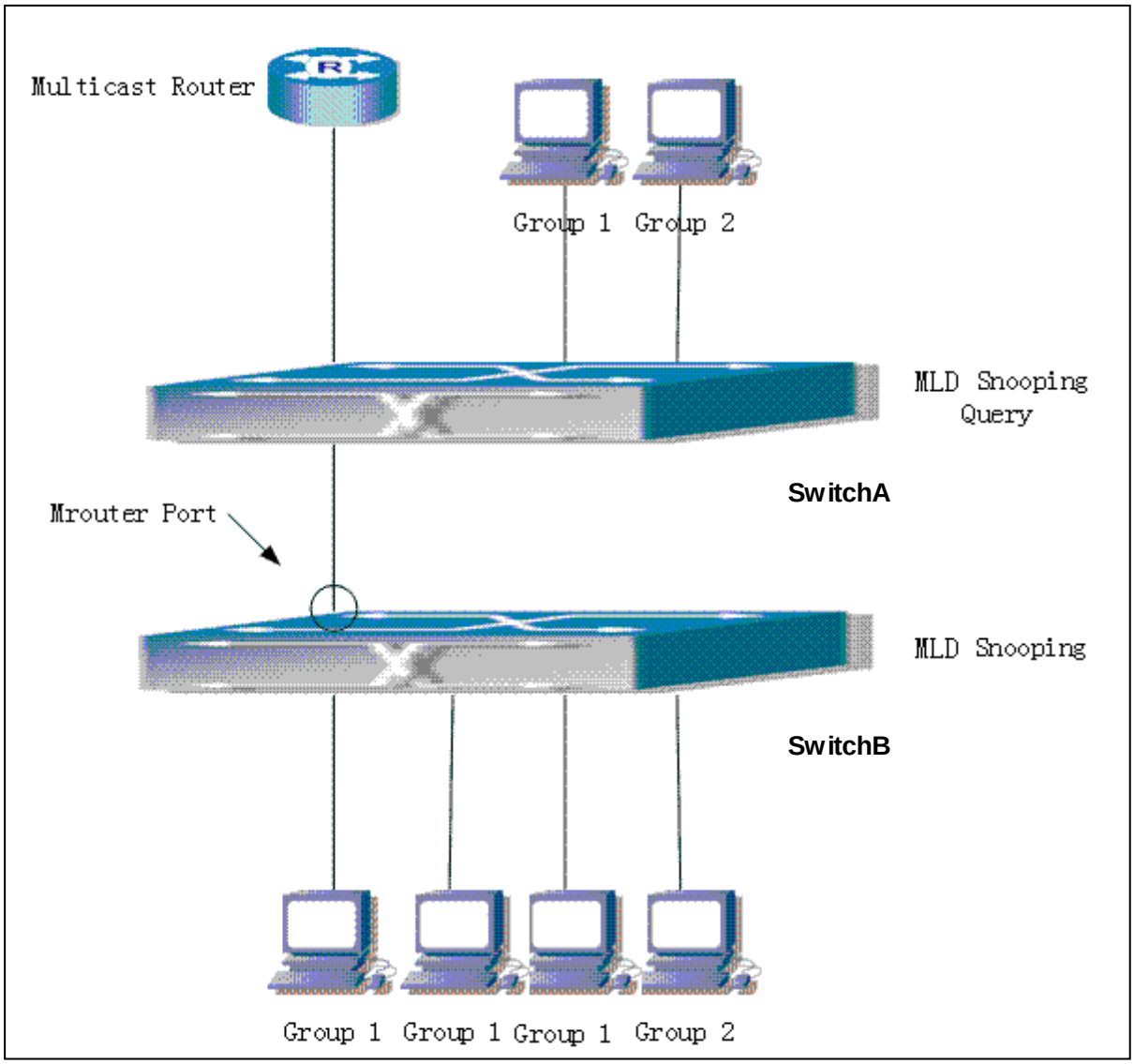


Fig 2-7 Switch as MLD Querier Function figure

Configuration of switch B is the same as the switches in case 1, and here the switch 1 replaces the Multicast Router in case 1. Assume the vlan 60 configured on it contains port 1, 2, 10 and 12, amongst port 1 is connected to multicast server, port 2 to switch2. To send Query periodically, global MLD Snooping has to be enabled while executing the mld snooping vlan 60 l2-general-querier, setting the vlan 60 to a Level 2 General Querier.

Configuration procedure is as follows:

SwitchA#config

SwitchA(config)#ipv6 mld snooping

SwitchA(config)#ipv6 mld snooping vlan 60

SwitchA(config)#ipv6 mld snooping vlan 60 l2-general-querier

SwitchB#config

SwitchB(config)#ipv6 mld snooping

SwitchB(config)#ipv6 mld snooping vlan 100
SwitchB(config)#ipv6 mld snooping vlan 100 mrouter interface ethernet 1/0/1
Multicast configuration:
Same as scenario 1
MLD Snooping interception results:
Same as scenario 1

Scenario 3: To run in cooperation with layer 3 multicast protocols

SWITCH which is used in Scenario 1 is replaced with ROUTER with specific configurations remains the same. And multicast and IGMP snooping configurations are the same with what it is in Scenario 1. To configure PIM-SM6 on ROUTER, and enable PIM-SM6 on vlan 100 (use the same PIM mode with the connected multicast router)

The configurations are listed as below:

switch#config
switch(config)#ipv6 pim multicast-routing
switch(config)#interface vlan 100
switch(config-if-vlan100)#ipv6 pim sparse-mode

MLD snooping does not distribute entries when layer 3 multicast protocol is enabled. It only does the following tasks.

- To remove the layer 2 multicast entries.
- To provide query functions to the layer 3 with vlan, S, and G as the parameters.
- When layer 3 MLD is disabled, re-enable distributing layer 2 multicast entries.

By looking up the layer 3 IP6MC entries, it can be found that ports can be indicated by the layer 3 multicast entries. This ensures the MLD Snooping can work in cooperation with the layer 3 multicast protocols.

2.7.4 MLD Snooping Troubleshooting

In configuring and using MLD Snooping, the MLD Snooping server may fail to run properly due to physical connection failure, wrong configuration, etc. The user should ensure the following:

- ☞ Ensure the physical connection is correct
- ☞ Ensure the MLD Snooping is enabled under global mode (using ipv6 mld snooping)
- ☞ Ensure the MLD Snooping is configured on the vlan under global mode (using ipv6 mld snooping vlan <vlan-id>)
- ☞ Ensure there is a vlan configured as a L2 general querier, or there is a static mrouter configured in a segment,

☞ Use command to check if the MLD snooping information is correct

Chapter 3 Multicast VLAN

3.1 Introductions to Multicast VLAN

Based on current multicast order method, when orders from users in different VLAN, each VLAN will copy a multicast traffic in this VLAN, which is a great waste of the bandwidth. By configuration of the multicast VLAN, we add the switch port to the multicast VLAN, with the IGMP Snooping/MLD Snooping functions enabled, users from different VLAN will share the same multicast VLAN. The multicast traffic only exists within a multicast VLAN, so the bandwidth is saved. As the multicast VLAN is absolutely separated from the user VLAN, security and bandwidth concerns can be met at the same time, after the multicast VLAN is configured, the multicast traffic will be continuously sent to the users.

3.2 Multicast VLAN Configuration Task List

1. Enable the multicast VLAN function
2. Configure the IGMP Snooping
3. Configure the MLD Snooping

1. Enable the multicast VLAN function

Command	Explanation
VLAN configuration mode	
multicast-vlan **no multicast-vlan**	Configure a VLAN and enable the multicast VLAN on it. The "**no multicast-vlan**" command disables the multicast function on the VLAN.
multicast-vlan association <*vlan-list*> **no multicast-vlan association <*vlan-list*>**	Associate a multicast VLAN with several VLANs. The no form of this command deletes the related VLANs associated with the multicast VLAN.
multicast-vlan association interface (ethernet | port-channel|) IFNAME **no multicast-vlan association interface (ethernet | port-channel|) IFNAME**	Associate the specified port with the multicast VLAN, so the associated ports are able to receive the multicast flow. The no command cancels the association between the ports and the multicast VLAN.

multicast-vlan mode {dynamic| compatible} **no multicast-vlan mode {dynamic| compatible}**	Configure the two modes of multicast vlan. The no command cancels the mode configuration.

2. Configure the IGMP Snooping

Command	Explanation
Global Mode	
ip igmp snooping vlan <*vlan-id*> **no ip igmp snooping vlan <*vlan-id*>**	Enable the IGMP Snooping function on the multicast VLAN. The no form of this command disables the IGMP Snooping on the multicast VLAN.
ip igmp snooping **no ip igmp snooping**	Enable the IGMP Snooping function. The no form of this command disables the IGMP snooping function.

3. **Configure the MLD Snooping**

ipv6 mld snooping vlan <*vlan-id*> **no ipv6 mld snooping vlan <*vlan-id*>**	Enable MLD Snooping on multicast VLAN; the no form of this command disables MLD Snooping on multicast VLAN.
ipv6 mld snooping **no ipv6 mld snooping**	Enable the MLD Snooping function. The no form of this command disables the MLD snooping function.

3.3 Multicast VLAN Examples

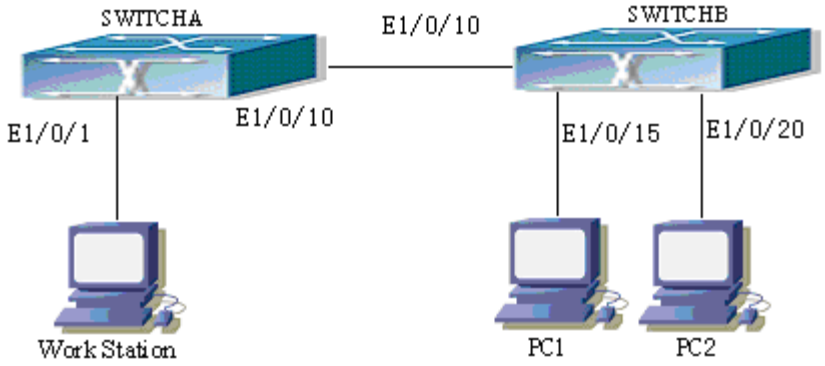


Fig 3-1 Function configuration of the Multicast VLAN

As shown in the figure, the multicast server is connected to the layer 3 switch switchA through port 1/0/1 which belongs to the VLAN10 of the switch. The layer 3 switch switchA

is connected with layer 2 switches through the port1/0/10, which configured as trunk port. On the switchB the VLAN100 is configured set to contain port1/0/15, and VLAN101 to contain port1/0/20. PC1 and PC2 are respectively connected to port 1/0/15 and1/0/20. The switchB is connected with the switchA through port1/0/10, which configured as trunk port. VLAN 20 is a multicast VLAN. By configuring multicast vlan, the PC1 and PC2 will receives the multicast data from the multicast VLAN.

Following configuration is based on the IP address of the switch has been configured and all the equipment are connected correctly.

Configuration procedure

```
SwitchA#config
SwitchA(config)#vlan 10
SwitchA(config-vlan10)#switchport access ethernet 1/0/1
SwitchA(config-vlan10)exit
SwitchA(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip pim dense-mode
Switch(Config-if-Vlan10)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan20)#exit
SwitchA(config)#interface vlan 20
SwitchA(Config-if-Vlan20)#ip pim dense-mode
SwitchA(Config-if-Vlan20)#exit
SwitchA(config)#ip pim multicast
SwitchA(config)# interface ethernet1/0/10
SwitchA(Config-If-Ethernet1/0/10)switchport mode trunk

SwitchB#config
SwitchB(config)#vlan 100
SwitchB(config-vlan100)#Switchport access ethernet 1/0/15
SwitchB(config-vlan100)exit
SwitchB(config)#vlan 101
SwitchB(config-vlan101)#Switchport access ethernet 1/0/20
SwitchB(config-vlan101)exit
SwitchB(config)# interface ethernet 1/0/10
SwitchB(Config-If-Ethernet1/0/10)#switchport mode trunk
SwitchB(Config-If-Ethernet1/0/10)#exit
SwitchB(config)#vlan 20
SwitchB(config-vlan20)#multicast-vlan
SwitchB(config-vlan20)#multicast-vlan association 100,101
```

```
SwitchB(config-vlan20)#exit
SwitchB(config)#ip igmp snooping
SwitchB(config)#ip igmp snooping vlan 20
```

When multicast VLAN supports IPv6 multicast, usage is the same with IPv4, but the difference is using with MLD Snooping, so does not give an example.