Edge-corE

Powered by Accton

ES4704(10)BD
Multicast
Management Guide

www.edge-core.com

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. All IPs in this chapter are IPv4.

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 datas 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 package, 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 ingressed 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 elsewise.

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. Neighbor 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、 Setup PIM-DM (Required)

2、 To configure static multicast routing entries(optional)

3、 Configure PIM-DM auxiliary parameters (Optional)

（1） Configure PIM-DM interface parameters

1) Configure PIM-DM hello message interval

2) Configure PIM-DM state-refresh origination-interval

3) To configure the boundary interfaces

4) To configure the management boundary

4、 3. Disable PIM-DM Protocol

1. Setup PIM-DM Protocol

The basic configuration to function PIM-DM routing protocol on EDGECORE series Layer 3 switch is very simple. It is only required to turn on PIM Multicast switch in Global Mode and turn on PIM-DM switch under corresponding interface.

Command	Explanation
Global Mode	
ip pim multicast-routing	Make PIM-DM Protocol on each interface to Enable status (but the commands below are required to really enable PIM-DM protocol on the interface)

And then turn on PIM-SM switch on the interface

Command	Explanation
Interface Configuration Mode	
ip pim dense-mode	Setup PIM-DM Protocol of the interface (Required)

2. To configure static multicast routing entries

Command	Notes
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 PIM-DM Sub-parameters

（1）Configure PIM-DM Interface Parameters

1）Configure PIM-DM hello message interval

Command	Explanation
Interface configuration mode	
ip pim hello-interval < *interval*> **no ip pim hello-interval**	Configure interface PIM-DM hello message interval; the "**no ip pim hello-interval**" command restores the default value.

2）Configure PIM-DM state-refresh origination-interval

Command	Explanation

Global Mode	
ip pim state-refresh origination-interval **no ip pim state-refresh origination-interval**	Configure the PIM-DM state-refresh message interval; the "**no ip pim state-refresh origination-interval**" command restores the default value.

3）To configure the boundary interfaces

Command	Notes
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.

4）To configure the management boundary

Command	Notes
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	Disable PIM-DM protocol on the interface
Global Mode	
no ip pim multicast-routing	Disable PIM-DM Protocol in global mode.

1.2.3 Command for PIM-DM

1.2.3.1 ip mroute

Command: 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>*]

Function: To configure static multicast entry. The no command is to delete some static multicast entries or some egress interfaces.

Parameter: <A.B.C.D> <A.B.C.D> are the source address and group address of multicast.

<ifname>, the first one is ingress interface, follow is egress interface.

Command Mode: Global Mode

Default: None.

Usage Guide: The <ifname> should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be fordwarded.

Example:

Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30

1.2.3.2 ip pim bsr-border

Command: ip pim bsr-border

no ip pim bsr-border

Function: To configure or delete PIM BSR BORDER interface.

Parameter: None.

Default: Non-BSR-BORDER

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the interface as the BSR-BORDER. If configured, BSR related messages will not received from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.

Example:

Switch(Config-if-Vlan1)#no ip pim bsr-border

Switch(Config-if-Vlan1)#

1.2.3.3 ip pim dense-mode

Command: ip pim dense-mode

no ip pim dense-mode

Function: Enable PIM-DM protocol on interface; the "**no ip pim dense-mode**" command

disenables PIM-DM protocol on interface.

Parameter: None.

Default: Disable PIM-DM protocol.

Command Mode: Interface Configure Mode

Usage Guide: The command will be taken effect, executing ip multicast-routing in Global Mode. Don't support multicast protocol mutual operation, namely can't synchronously enable dense mode and sparse mode in one swtich.

Example: Enable PIM-DM protocol on interface vlan1.

Switch (config)#ip pim multicast-routing

Switch (config)#interface vlan 1

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

1.2.3.4 ip pim dr-priority

Command: ip pim dr-priority <*priority*>

no ip pim dr-priority

Function: Configure,disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "**no ip pim dr-priority"** command restores the default value.

Parameter: <*priority*> is priority

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Range from 0 to 4294967294, the higher value has more priority.

Example: Configure vlan's DR priority to 100

Switch (config)# interface vlan 1

Switch(Config-if-Vlan1)ip pim dr-priority 100

Switch (Config -if-Vlan1)#

1.2.3.5 ip pim exclude-genid

Command: ip pim exclude-genid

no ip pim exclude-genid

Function: This command makes the Hello packets sent by PIM SM do not include GenId option. The "**no ipv6 pim exclude-genid**" command restores the default value

Parameter: None

Default: The Hello packets include GenId option.

Command Mode: Interface Configuration Mode

Usage Guide: This command is used to interact with older Cisco IOS version.

Example: Configure the Hello packets sent by the switch do not include GenId option.

Switch (Config-if-Vlan1)#ip pim exclude-genid

Switch (Config-if-Vlan1)#

1.2.3.6 ip pim hello-holdtime

Command: ip pim hello-holdtime <*value*>

no ip pim hello-holdtime

Function: Configure or disable the Holdtime option in the Hello packets,this value is to describe neighbore holdtime,if the switch hasn't received the neighbore hello packets when the holdtime is over, this neighbore is deleted. The "**no ip pim hello-holdtime**" command cancels configured holdtime value and restores default value.

Parameter: <*value*> is the value of holdtime.

Default: The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is 30s,so Holdtime's default value is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval , this configuration is denyed. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval,hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained.

Example: Configure vlan1's Hello Holdtime

Switch (config)# interface vlan1

Switch (Config -if-Vlan1)#ip pim hello-holdtime 10

Switch (Config -if-Vlan1)#

1.2.3.7 ip pim hello-interval

Command: ip pim hello-interval < *interval*>

no ip pim hello-interval

Function: Configure interface PIM-DM hello message interval; the "**no ip pim hello-interval**" restores default value.

Parameter: < *interval*> is interval of periodically transmitted PIM-DM hello message, value range from 1s to 18724s.

Default: Default interval of periodically transmitted PIM-DM hello message as 30s.

Command Mode: Interface Configuration Mode.

Usage Guide: Hello message makes PIM-DM switch mutual location, and ensures neighborship. PIM-DM switch announces existence itself by periodically transmitting hello messages to neighbors. If it doesn't receive hello messages from neighbors in regulation time, it confirms that the neighbors were lost. Configuration time is not more than neighbor overtime.

Example: Configure PIM-DM hello interval on interface vlan1.

Switch (config)#interface vlan1

Switch(Config-if-Vlan1)#ip pim hello-interval 20

1.2.3.8 ip pim multicast-routing

Command: ip pim multicast-routing

no ip pim multicast-routing

Function: Enable PIM-SM globally. The "**no ip pim multicast-routing** » command disables PIM-SM globally.

Parameter: None

Default: Disabled PIM-SM

Command Mode: Global Mode

Usage Guide: Enable PIM-SM globally.The interface must enable PIM-SM to have PIM-SM work

Example: Enable PIM-SM globally.

Switch (config)#ip pim multicast-routing

1.2.3.9 ip pim neighbor-filter

Command: ip pim neighbor-filter{<*list-number*>}

no ip pim neighbor-filter{<*list-number*>}

Function: Configure the neighbore access-list. If filtered by the lists and connections with neighbors are created, this connections are cut off immediately. If no connection is created, this conncetion can't be created.

Parameter: <*list-number*>: <*list-number*> is the simple access-list number, it ranges from 1 to 99

Default: No neighbor filter configuration.

Command Mode: Interface Configuration Mode

Usage Guide: ACL's default is DENY. If configuring access-list 1,access-list 1's default is deny. In the following example, if "permit any-source" is not configured, deny 10.1.4.10 0.0.0.255 is the same as deny any-source.

Example: Configure vlan's filtering rules of pim neighbors.

Switch #show ip pim neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
10.1.4.10	Vlan1	02:30:30/00:01:41	v2	4294967294 / DR

Switch (Config-if-Vlan1)#ip pim neighbor-filter 2

Switch (config)#access-list 2 deny 10.1.4.10 0.0.0.255

Switch (config)#access-list 2 permit any-source

Switch (config)#show ip pim neighbor

Switch (config)#

1.2.3.10 ip pim scope-border

Command: ip pim scope-border [*<1-99 >*|*<acl_name>*]

no ip pim scope-border

Function: To configure or delete management border of PIM.

Parameters: <1-99> is the ACL number for the management border.

<acl_name> is the ACL name for the management border.

Default: Not management border. If no ACL is specified, the default management border will be used.

Command Mode: Interface Configuration Mode

Usage Guide: To configure the management border and the ACL for the PIM protocol. The multicast data flow will not be forwarded to the SCOPE-BORDER.

Example:

Switch(Config-if-Vlan2)#ip pim scope-border 3

Switch(Config-if-Vlan2)#

1.2.3.11 ip pim state-refresh origination-interval

Command: ip pim state-refresh origination-interval *<interval>*

no ip pim state-refresh origination-interval

Function: Configure transmission interval of state-refresh message. The "**no ip pim state-refresh origination-interval**" command restores default value.

Parameter: <*interval*> packet transmission interval value is from 4s to 100s.

Default: 60s

Command Mode: Global Mode

Usage Guide: The first-hop router periodically transmits stat-refresh messages to maintain PIM-DM list Items of all the downstream routers. The command can modify origination interval of state-refresh messages. Usually do not modify relevant timer interval.

Example: Configure transmission interval of state-refresh message to 90s.

Switch (config)#ip pim state-refresh origination-interval 90

1.2.4 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.

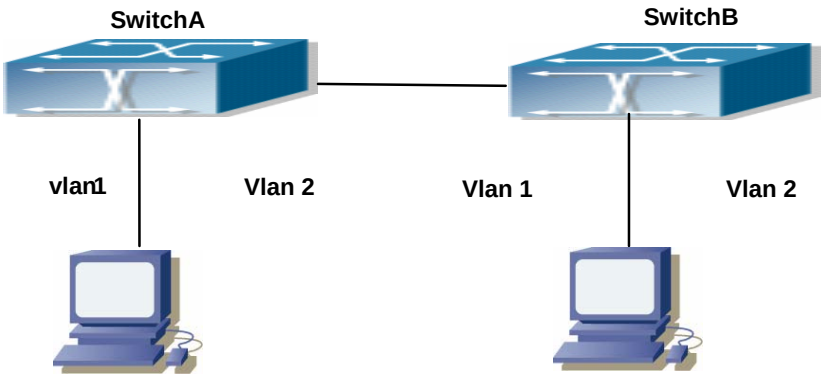


Fig 1-1 PIM-DM Typical Environment

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.

1.2.5 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 toTechnology Service Center.

1.2.5.1 Monitor and debug command

1.2.5.1.1 debug pim timer sat

Command: debug pim timer sat

no debug pim timer sat

Function: Enable debug switch of PIM-DM source activity timer information in detail; the "**no debug pim timer sat**" command disenables the debug switch.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: Enable the switch, and display source activity timer information in detail.

Example: Switch # debug ip pim timer sat

Remark: Other debug switches in PIM-DM are common in PIM-SM, including debug pim event, debug pim packet, debug pim nexthop, debug pim mib, debug pim nsm, debug pim mfc, debug pim timer, debug pim state, refer to PIM-SM handbook.

1.2.5.1.2 debug pim timer srt

Command: debug pim timer srt

no debug pim timer srt

Function: Enable debug switch of PIM-DM state-refresh timer information in detail; the "**no debug pim timer srt**" command disenables the debug switch.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode and Global Mode.

Usage Guide: Enable the switch, and display PIM-DM state-refresh timer information in detail.

Example: Switch # debug ip pim timer srt

Remark: Other debug switches in PIM-DM are common in PIM-SM, including debug pim event,

debug pim packet, debug pim nexthop, debug pim nsm, debug pim mfc, debug pim timer, debug pim state, refer to PIM-SM manual section.

1.2.5.1.3 show ip mroute

Command: show ip mroute [<GroupAddr> [<SourceAddr>]]

Function: show IPv4 software multicast route table.

Parameter: GroupAddr: show the multicast entries relative to this Group address.

SourceAddr：show the multicast route entries relative to this source address.

Default: None

Command Mode： Admin mode and global mode

Usage Guide:

Example: show all entries of multicast route table

Switch(config)#show ip mroute

Name: Loopback, Index: 2002, State:49

Name: null0, Index: 2003, State:49

Name: sit0, Index: 2004, State:80

Name: Vlan1, Index: 2005, State:1043

Name: Vlan2, Index: 2006, State:1002

Name: pimreg, Index: 2007, State:c1

The total matched ipmr active mfc entries is 1, unresolved ipmr entries is 0

Group	Origin	Iif	Wrong	Oif:TTL
225.1.1.1	192.168.1.136	vlan1	0	2006:1

Displayed information	Explanation
Name	the name of interface
Index	the index number of interface
State	the state of interface
The total matched ipmr active mfc entries	The total matched active IP multicast route mfc（multicast forwarding cache） entries
unresolved ipmr entries	unresolved ip multicast route entries
Group	the destination address of the entries
Origin	the source address of the entries
Iif	ingress interface of the entries
Wrong	packets received from the wrong interface
Oif	egress interface of the entries
TTL	the value of TTL

Remark: This command is common in PIM-SM and DVMRP.

1.2.5.1.4 show ip pim interface

Command: show ip pim interface

Function: Display PIM interface information

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display PIM interface information

Example: Switch (config)#show ip pim interface

Address	Interface	VIFindex	Ver/ Mode	Nbr Count	DR Prior	DR
10.1.4.3	Vlan1	0	v2/S	1	1	10.1.4.3
10.1.7.1	Vlan2	2	v2/S	0	1	10.1.7.1

Displayed Information	Explanations
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count	The interface's neighbor count
DR Prior	Dr priority
DR	The interface's DR address

1.2.5.1.5 show ip pim mroute dense-mode

Command: show ip pim mroute dense-mode [group <*A.B.C.D*>] [source <*A.B.C.D*>]

Function: Display PIM-DM message forwarding items.

Parameter:group <A.B.C.D>: displays forwarding items relevant to this multicast address.

Source <A.B.C.D>: displays forwarding items relevant to this source.

Default: Do not display (Off).

Command Mode: Admin Mode

Usage Guide: The command shows PIM-DM multicast forwarding items, namely forwarding items of forward multicast packet in system FIB table.

Example: Display all of PIM-DM message forwarding items.

Switch(config)#show ip pim mroute dense-mode

IP Multicast Routing Table

(*,G) Entries: 1

(S,G) Entries: 1

(*, 226.0.0.1)

Local

(192.168.1.12, 226.0.0.1)

RPF nbr: 0.0.0.0

RPF idx: Vlan2

Upstream State: FORWARDING

Origin State: ORIGINATOR

Local

Pruned

Asserted

Outgoing

Switch#

Displayed Information	Explanations
(*,226.0.0.1)	(*,G) Forwaridng item
(192.168.1.12, 226.0.0.1)	(S,G) Forwarding item
RPF nbr	Backward path neighbor, upstream neighbor of source direction in DM, 0.0.0.0 expresses the switch is the first hop.
RPF idx	Interface located in RPF neighbor
Upstream State	Upstream direction, including FORWARDING(forwarding upstream data), PRUNED(Upstream stops forwarding data), ACKPENDING(waiting for upstream response, forwarding upstream data)
Origin State	The two states: ORIGINATOR(on transmit state-refresh state), NON_ORIGINATOR(on non_transmit state-refresh state)
Local	Local position joins interface, the interface receives IGMP Join
Pruned	PIM prunes interface, the interface receives Prune messages
Asserted	Asserted state
Outgoing	Multicast data finally exported from interface is index number, index is 2 in this case. It can check interface information in detail by commanding show ip pim interface

1.2.5.1.6 show ip pim neighbor

Command: show ip pim neighbor

Function: Display router neighbors

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display multicast router neighbors maintained by the PIM

Example: Switch (config)#show ip pim neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
10.1.6.1	Vlan1	00:00:10/00:01:35	v2	1 /
10.1.6.2	Vlan1	00:00:13/00:01:32	v2	1 /
10.1.4.2	Vlan3	00:00:18/00:01:30	v2	1 /
10.1.4.3	Vlan3	00:00:17/00:01:29	v2	1 /

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Neighbor interface
Uptime/Expires	Running time /overtime
Ver	Pim version ,v2 usually
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP.

1.2.5.1.7 show ip pim nexthop

Command: show ip pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the PIM buffered nexthop router information.

Example:

Switch(config)#show ip pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable

Destination Addr	Type	Nexthop Num	Nexthop Ifindex	Nexthop Name	Nexthop	Metric	Pref	Refcnt
192.168.1.1	N...	1	0.0.0.0	2006	0	0	1	
192.168.1.9	..S.	1	0.0.0.0	2006	0	0	1	

Displayed Information	Explanations

Destination	Destination of next item
Type	N: created nexthop,RP direction and S direction are not determined . R: RP derection S: source direction U: can't reach
Nexthop Num	Nexthop number
Nexthop Addr	Nexthop address
Nexthop Ifindex	Nexthop interface index
Nexthop Name	Nexthop name
Metric	Metric Metric to nexthop
Pref	Preference Route preference
Refcnt	Reference count

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 bandwith 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、 To configure static multicast routing entries(required)

3、 Configure PIM-SM sub-parameters (Optional)

（1） Configure PIM-SM interface parameters

1) Configure PIM-SM hello message interval
2) Configure interface as PIM-SM domain boundary
3) To configure the interface as the boundary interface of the PIM-SM protocol
4) To configure the interface as the management boundary of the PIM-SM protocol

（2） Configure PIM-SM global parameters

1) Configure Switch as candidate BSR
2) Configure switch as candidate RP

4、 Disable PIM-SM Protocol

1. Enable PIM-SM Protocol

The basic configuration to function PIM-SM Routing Protocol on EDGECORE series Layer 3 switch is very simple. It is only required to turn on PIM Multicast switch in Global Mode and turn on PIM-SM switch under corresponding interface.

Command	Explanation
Global Mode	
ip pim multicast-routing	Make PIM-SM Protocol on each interface to Enable status (but the commands below are required to really enable PIM-SM protocol on the interface) (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. To configure static multicast routing entries

Command	Notes
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 PIM-SM Sub-parameters

（1）Configure PIM-SM Interface Parameters

1）Configure PIM-SM hello message interval

Command	Explanation
Interface Configuration Mode	
ip pim hello-interval < *interval*> **no ip pim hello-interval**	Configure interface PIM-SM hello message interval; the "**no ip pim hello-interval**" command restores the default value.

2）Configure PIM-SM hello message holdtime

Command	Explanation
Interface Configuration Mode	
ip pim hello-holdtime <*value*> **no ip pim hello-holdtime**	Configure the value of holdtime field in interface PIM-SM hello message.

3）Configure PIM-SM Neighbor Access-list

Command	Explanation
Interface Configuration Mode	
[no] ip pim neighbor-filter{<*access-list-number*> }	Configure Neighbor Access-list. If a neighbor is filtered by the list and a connection has been set up with this neighbor, then this connection is cut off immediately; and if no connection is set up yet, then this connection can't be created.

4）To configure the interface as the boundary interface of the PIM-SM protocol

Command	Notes
Interface configuration	
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）To configure the interface as the management boundary of the PIM-SM protocol

Command	Notes
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 PIM-SM Global Parameters

1) Configure switch to be candidate BSR

Command	Explanation
Global 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 BSRs. The "**no ip pim bsr-candidate**" command cancels the configuration of BSR.

2) Configure switch to be candidate RP

Command	Explanation
Global Mode	
ip pim rp-candidate { vlan <*vlan-id* >| <*ifname*>} [<A.B.C.D/M>][<*priority*>] **(no) ip pim rp-candidate**	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 RPs. The "**no ip pim rp-candidate**" command cancels the configuration of RP.

3) Configure Static RP

Command	Explanation
Global 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>}**	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 RPs. The "**no ip pim rp-address <A.B.C.D> {<*all*>|<A.B.C.D/M>}**" command cancels the configuration of RP.

4.Disable PIM-SM Protocol

Command	Explanation
Interface Configuration Mode	
no ip pim sparse-mode | no ip pim multicast-routing **no ip pim sparse-mode | no ip pim multicast-routing (Global Mode)**	Disable PIM-SM Protocol.

1.3.3 Command For PIM-SM

1.3.3.1 ip mroute

Command: 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*>]

Function: To configure static multicast entry. The no command is to delete some static multicast entries or some egress interfaces.

Parameter: <A.B.C.D> <A.B.C.D> are the source address and group address of multicast.

<ifname>, the first one is ingress interface, follow is egress interface.

Command Mode: Global Mode

Default: None.

Usage Guide: The <ifname> should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be fordwarded.

Example:

Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30

1.3.3.2 ip pim accept-register

Command: ip pim accept-register list <*list-number*>

no ip pim accept-register

Function: Filter the specified multicast group and multicast address.

Parameter: <***list-number***>: is the access-list number ,it ranges from 100 to 199.

Default: Permit the multicast registers from any sources to any groups.

Command Mode: Global Mode

Usage Guide: This command is used to configure the access-list filtering the PIM REGISTER packets.The addresses of the access-list respectively indicate the filtered multicast sources and multicast groups' information. For the source-group combinations that match DENY, PIM sends REGISTER-STOP immediately and does not create group records when receiving REGISTER packets.Unlike other access-list,when the access-list is configured ,the default value is PERMIT.

Example: Configure the filtered register message's rule to myfilter.

Switch(config)#ip pim accept-register list 120

Switch (config)#access-list 120 deny ip 10.1.0.2 0.0.0.255 239.192.1.10 0.0.0.255

1.3.3.3 ip pim bsr-border

Command: ip pim bsr-border

no ip pim bsr-border

Function: To configure or delete PIM BSR BORDER interface.

Parameter: None.

Default: Non-BSR-BORDER

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the interface as the BSR-BORDER. If configured, BSR related messages will not received from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.

Example:

Switch(Config-if-Vlan1)#no ip pim bsr-border

Switch(Config-if-Vlan1)#

1.3.3.4 ip pim bsr-candidate

Command:ip pim bsr-candidate {vlan <*vlan-id*>| <*ifname*>} [*hash-mask-length*] [*priority*]

no ip pim bsr-candidate

Function: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. The command **"no ip pim bsr-candidate"** disables the candidate BSR.

Parameter: ***Ifname*** is the specified interface's name;

[*hash-mask-length*] is the specified hash mask length.It's used for the RP enable selection and ranges from 0 to 32;

[*priority*] is the candidate BSR priority and ranges from 0 to 255. If this parameter is not

configured ,the default priority value is 0.

Default: This switch is not a candidate BSR router.

Command Mode: Global Mode

Usage Guide: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. Only this command is configured , this switch is the BSR candidate router.

Example: Globally configure the interface vlan1 as the candidate BSR-message transmitting interface.

Switch (config)# ip pim bsr-candidate vlan1 30 10

1.3.3.5 ip pim cisco-register-checksum

Command: ip pim cisco-register-checksum [group-list <*simple-acl*>]

no ip pim cisco-register-checksum [group-list <*simple-acl*>]

Function: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

Default: Compute the checksum according to the regester packets's head length, default: 8

Parameter: <*simple-acl*>: <1-99> Simple access-list **<*simple-acl*>:** <1-99> Simple access-list

Command Mode: Global Mode

Usage Guide: This command is uesd to interact with older Cisco IOS version.

Example: Configure the register packet's ckecksum of the group specified by myfilter to use the whole packet's length.

Switch (config)#ip pim cisco-register-checksum group-list 23

1.3.3.6 ip pim dr-priority

Command: ip pim dr-priority <*priority*>

no ip pim dr-priority

Function: Configure,disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "**no ip pim dr-priority"** command restores the default value.

Parameter: <*priority*> is priority

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Range from 0 to 4294967294, the higher value has more priority.

Example: Configure vlan's DR priority to 100

Switch (config)# interface vlan 1

Switch(Config-if-Vlan1)ip pim dr-priority 100

Switch (Config -if-Vlan1)#

1.3.3.7 ip pim exclude-genid

Command: ip pim exclude-genid

no ip pim exclude-genid

Function: This command makes the Hello packets sent by PIM SM do not include GenId option. The "**no ipv6 pim exclude-genid**" command restores the default value

Parameter: None

Default: The Hello packets include GenId option.

Command Mode: Interface Configuration Mode

Usage Guide: This command is used to interact with older Cisco IOS version.

Example: Configure the Hello packets sent by the switch do not include GenId option.

Switch (Config-if-Vlan1)#ip pim exclude-genid

Switch (Config-if-Vlan1)#

1.3.3.8 ip pim hello-holdtime

Command: ip pim hello-holdtime <*value*>

no ip pim hello-holdtime

Function: Configure or disable the Holdtime option in the Hello packets,this value is to describe neighbore holdtime,if the switch hasn't received the neighbore hello packets when the holdtime is over, this neighbore is deleted. The "**no ip pim hello-holdtime**" command cancels configured holdtime value and restores default value.

Parameter: <*value*> is the value of holdtime.

Default: The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is 30s,so Holdtime's default value is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval , this configuration is denyed. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval,hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained.

Example: Configure vlan1's Hello Holdtime

Switch (config)# interface vlan1

Switch (Config -if-Vlan1)#ip pim hello-holdtime 10

Switch (Config -if-Vlan1)#

1.3.3.9 ip pim hello-interval

Command: ip pim hello-interval <*interval*>

no ip pim hello-interval

Function: Configure the interface's hello_interval of pim hello packets. The "**no ip pim hello-interval**" command restores the default value.

Parameter: <*interval*> is the hello_interval of periodically transmitted pim hello packets', ranges from 1 to 18724s.

Default: The default periodically transmitted pim hello packets' hello_interval is30s.

Command Mode: Interface Configuration Mode

Usage Guide: Hello messages make pim switches oriente each other and determine neighbore relationship. Pim switch annouce the existance of itself by periodically transmitting hello messages to neighbores. If no hello messages from neighores are received in the certain time, the neighbore is considered lost. This value can't be greater than neighbore overtime.

Example: Configure vlan's pim-sm hello interval

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip pim hello-interval 20

Switch(Config-if-Vlan1)#

1.3.3.10 ip pim ignore-rp-set-priority

Command: ip pim ignore-rp-set-priority

no ip pim ignore-rp-set-priority

Function: When RP selection is carried out, this command configure the switch to enable Hashing regulation and ignore RP priority. This command is used to interact with older Cisco IOS versions.

Default: Disabled

Parameter: None

Command Mode: Global Mode

Usage Guide: When selecting RP, Pim usually will select according to RP priority. When this command is configured, pim will not select according to RP priority. Unless there are older routers in the net, this command is not recommended.

Example: Switch (config)#ip pim ignore-rp-set-priority

1.3.3.11 ip pim jp-timer

Command: ip pim jp-timer <*value*>

no ip pim jp-timer

Function: Configure to add JP timer.the "**no ip pim jp-timer**" command restores the default value.

Parameter: <*value*> ranges from 10 to 65535s

Default: 60s

Command Mode: Global Mode

Usage Guide: Configure the interval of JOIN-PRUNE packets sent by PIM periodically, the default value is 60s. The default value is recommended if no special reasons.

Example: Configure the interval of jt timer

Switch (config)#ip pim jp-timer 59

1.3.3.12 ip pim multicast-routing

Command: ip pim multicast-routing

no ip pim multicast-routing

Function: Enable PIM-SM globally. The "**no ip pim multicast-routing** » command disables PIM-SM globally.

Parameter: None

Default: Disabled PIM-SM

Command Mode: Global Mode

Usage Guide: Enable PIM-SM globally.The interface must enable PIM-SM to have PIM-SM work

Example: Enable PIM-SM globally.

Switch (config)#ip pim multicast-routing

1.3.3.13 ip pim neighbor-filter

Command: ip pim neighbor-filter <*list-number*>

no ip pim neighbor-filter <*list-number*>

Function: Configure the neighbore access-list. If filtered by the lists and connections with neighbors are created, this connections are cut off immediately. If no connection is created, this conncetion can't be created.

Parameter: <*list-number*>: the simple access-list number, it ranges from 1 to 99

Default: No neighbor filter configuration.

Command Mode: Interface Configuration Mode

Usage Guide: ACL's default is DENY. If configuring access-list 1,access-list 1's default is deny. In the following example, if "permit any-source" is not configured, deny 10.1.4.10 0.0.0.255 is the same as deny any-source.

Example: Configure vlan's filtering rules of pim neighbors.

Switch #show ip pim neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
10.1.4.10	Vlan1	02:30:30/00:01:41	v2	4294967294 / DR

Switch (Config-if-Vlan1)#ip pim neighbor-filter 2

Switch (config)#access-list 2 deny 10.1.4.10 0.0.0.255

Switch (config)#access-list 2 permit any-source
Switch (config)#show ip pim neighbor
Switch (config)#

1.3.3.14 ip pim register-rate-limit

Command: ip pim register-rate-limit <*limit*>
no ip pim register-rate-limit
Function: This command is used to configure the speedrate of DR sending register packets; the unit is packet/second. The "**no ip pim Register-rate-limit**" command restores the default value. This configured speedrate is each（S, G）state's ,not the whole system's.
Parameter: <*limit*> ranges from 1 to 65535.
Default: No limit for sending speed
Command Mode: Global Mode
Usage Guide: This configuration is to prevent the attack to DR, limiting sending REGISTER packets.
Example: Configure the speedrate of DR sending register packets to 59 p/s.
Switch (config)#ip pim register-rate-limit 59

1.3.3.15 ip pim register-rp-reachability

Command: ip pim register-rp-reachability
no ip pim register-rp-reachability
Function: This command makes DR check the RP reachability in the process of registration.
Parameter: None
Default: Do not check
Command Mode: Global Mode
Usage Guide: This command configures DR whether or not to check the RP reachability.
Example: Configure DR to check the RP reachability.
Switch (config)#ip pim register-rp-reachability

1.3.3.16 ip pim register-source

Command:ip pim register-source {<*A.B.C.D*> | <*ifname*> | <*ethernet*> | vlan <*vlan-id*>}
no ip pim register-source
Function: This command is to configure the source address of register packets sent by DR to overwrite default source address. This default source address is uaually the RPF neighbor of source host direction.
Parameter: <*ifname*> is the interface name,
<*ethernet*> is the ethernet interface,

<vlan-id> is VLAN ID;

<A.B.C.D> is the configured source IP addresses.

Default: Do not check

Command Mode: Global Mode

Usage Guide: The "**no ip pim register-source**" command restores the default value,no more parameter is needed. Configured address must be reachable to Register-Stop messages sent by RP. It's usually a circle address, but it can be other physical addresses. This address must be announcable through unicast router protocols of DR.

Example: Configure the source address sent by DR.

Switch (config)#ip pim register-source 10.1.1.1

1.3.3.17 ip pim register-suppression

Command: ip pim register-suppression <*value*>

no ip pim register-suppression

Function: This command is to configure the value of register suppression timer,the unit is second. The "**no ip pim register-suppression**" command restores the default value.

Parameter: <***value***> is the timer's value,it ranges from 10 to 65535s.

Default: 60s

Command Mode: Global Mode

Usage Guide: If this value is configured at DR,it's the value of register suppression timer; The bigger one of the default register keep-alive time of RP (210s) and the sum of triple register suppression time and 5. If configure this value on RP without the command "ip pim rp-register-kat", this command may modify the RP register keep-alive time.

Example: Configure the value of register suppression timer to 10s.

Switch(config)#ip pim register- suppression 10

1.3.3.18 ip pim rp-address

Command: ip pim rp- address <*A.B.C.D*> <*A.B.C.D/M*>

no ip pim rp-address <*A.B.C.D*> [<*A.B.C.D/M*>|<*all*>]

Function: This command is to configure static RP globally or in a multicast address range. The **"no ipv6 pim rp-address <*A.B.C.D*> [<*A.B.C.D/M*>|<*all*>]**" command cancels static RP.

Parameter: <*A.B.C.D*> is the RP address

<A.B.C.D/M> the scope of the specified RP address

<all> is all the range

Default: This switch is not a RP static router.

Command Mode: Global Mode

Usage Guide: This command is to configure static RP globally or in a multicast address range and configure PIM-SM static RP information. Attention, when computing rp, BSR RP is selected

first.If it dosen't succeed, static RP is selected.

Example: Configure vlan1 as candidate RP announcing sending interface globally.

Switch (config)# ip pim rp-address 10.1.1.1 238.0.0.0/8

Switch (config)#

1.3.3.19 ip pim rp-candidate

Command: ip pim rp-candidate { vlan < *vlan-id* >| <*ifname*>} [<*A.B.C.D/M*>] [<priority>]

no ip pim rp-candiate

Function: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs. The "**no ip pim rp-candiate**" command cancels the candidate RP.

Parameter: *vlan-id* is**Vlan ID;**

ifname is the name of the specified interface;

A.B.C.D/M is the ip prefix and mask;

<priority> is the RP selection priority, it ranges from 0 to 255, the default value is 192, the lower value has more priority.

Default: This switch is not a RP static router.

Command Mode: Global Mode

Usage Guide: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs.Only this command is configured,this switch is the RP candidate router.

Example: Configure vlan1 as the sending interface of candidate RP announcing sending messages

Switch (config)# ip pim rp-candidate vlan1 100

1.3.3.20 ip pim rp-register-kat

Command: ip pim rp-register-kat <*vaule*>

no ip pim rp-register-kat

Function: This command is to congifure the KAT（KeepAlive Timer）value of the RP（S, G）items,the unit is second. The "**no ip pim rp-register-kat**" command restores the default value.

Parameter: <*vaule*> is the timer value,it ranges from 1 to 65535s.

Default: 185s

Command Mode: Global Mode

Usage Guide: This command is to configure the RP's keepalive time,during the keepalive time RP's （S,G）item will not be deleted because it hasn't received REGISTER packets. If no new REGISTER packet is received when the keepalive time is over, this item will be obsoleted.

Example: Configure the kat value of RP's (S,G) item to 180s

Switch (config)#ip pim rp-register- kat 180

1.3.3.21 ip pim scope-border

Command: ip pim scope-border [<*1-99* >|<*acl_name*>]

no ip pim scope-border

Function: To configure or delete management border of PIM.

Parameters: <1-99> is the ACL number for the management border.

<acl_name> is the ACL name for the management border.

Default: Not management border. If no ACL is specified, the default management border will be used.

Command Mode: Interface Configuration Mode

Usage Guide: To configure the management border and the ACL for the PIM protocol. The multicast data flow will not be forwarded to the SCOPE-BORDER.

Example:

Switch(Config-if-Vlan2)#ip pim scope-border 3

Switch(Config-if-Vlan2)#

1.3.3.22 ip pim sparse-mode

Command: ip pim sparse-mode [passive]

no ip pim sparse-mode [passive]

Function: Enable PIM-SM on the interface; the "**no ip pim sparse-mode [passive]**" command disables PIM-SM.

Parameter: [*passive*] means to disable PIM-SM (that's PIM-SM doesn't receive any packets) and only enable IGMP(reveice and transmit IGMP packets).

Default: Do not enable PIM-SM

Command Mode: Interface Configuration Mode

Usage Guide: Enable PIM-SM on the interface.

Example: Enable PIM-SM on the interface vlan1.

Switch (config)#interface vlan 1

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

Switch(Config-if-Vlan1)#

1.3.3.23 ip multicast ssm

Command: ip multicast ssm {default|range <*access-list-number* >}

no ip multicast ssm

Function: Configure the range of pim ssm multicast address. The "**no ip multicast ssm**" command deletes configured pim ssm multicast group.

Parameter: *default :* indicates the default range of pim ssm multicast group is 232/8.

<access-list-number > is the applying access-list number, it ranges from 1 to 99.

Default: Do not configure the range of pim ssm group address

Command Mode: Global Mode

Usage Guide:

1. Only this command is configured, pim ssm can be available.

2. Before configuring this command, make sure ip pim multicasting succeed. This command can't work with DVMRP.

3. Access-list can't used the lists created by ip access-list, but the lists created by access-list.

4.Users can execute this command first and then configure the corresponding acl; or delete corresponding acl in the bondage. After the bondage, only command no ip multicast ssm can release the bondage.

5 .If ssm is needed, this command should be configured at the related edge route. For example, the local switch with igmp(must) and multicast source DR or RP(at least one of the two) configure this command, the middle switch need only enable PIM-SM.

Example: Configure the switch to enable PIM-SSM, the group's range is what is specified by access-list 23.

Switch (config)#ip multicast ssm range 23

1.3.4 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.

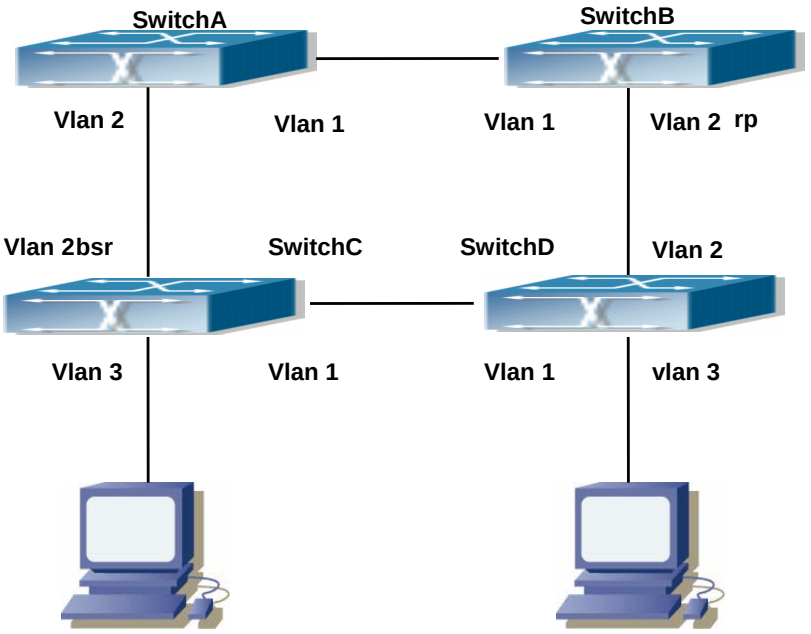


Fig 1-2 PIM-SM Typical Environment

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.

1.3.5 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 toTechnology Service Center.

1.3.5.1 Monitor And Debug Command

1.3.5.1.1 debug pim event

Command: debug pim event
no debug pim event
Function: Enable or Disable pim event debug switch
Parameter: None
Default: Disabled
Command Mode: Admin Mode.
Usage Guide: Enable pim event debug switch and display events information about pim operation.
Example: Switch# debug ip pim event

1.3.5.1.2 debug pim mfc

Command: debug pim mfc
no debug pim mfc
Function: Enable or Disable pim mfc debug switch
Parameter: None
Default: Disabled
Command Mode: Admin Mode.
Usage Guide: Enable pim mfc debug switch and display generated and transmitted multicast id's information.
Example: Switch# debug ip pim mfc

1.3.5.1.3 debug pim mib

Command: debug pim mib

no debug pim mib

Function: Enable or Disable PIM MIB debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode and Global Mode

Usage Guide: Inspect PIM MIB information by PIM MIB debug switch. It's not available now and it's for the future extension.

Example: Switch# debug ip pim mib

1.3.5.1.4 debug pim nexthop

Command: debug pim nexthop

no debug pim nexthop

Function: Enable or Disable pim nexthop debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect PIM NEXTHOP changing information by the pim nexthop switch.

Example: Switch# debug ip pim nexthop

1.3.5.1.5 debug pim nsm

Command: debug pim nsm

no debug pim nsm

Function: Enable or Disable pim debug switch communicating with Network Services

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the communicating information between PIM and Network Services by this switch.

Example: Switch# debug ip pim nsm

1.3.5.1.6 debug pim packet

Command:debug pim packet

debug pim packet in

debug pim packet out

no debug pim packet

no debug pim packet in

no debug pim packet out

Function: Enable or Disable pim debug switch

Parameter: in display only received pim packets

out display only transmitted pim packets

none display both

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the received and transmitted pim packets by this switch.

Example: Switch# debug ip pim packet in

1.3.5.1.7 debug pim state

Command: debug pim state

no debug pim state

Function: Enable or Disable pim debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the changing information about pim state by this switch.

Example: Switch# debug ip pim state

1.3.5.1.8 debug pim timer

Command: debug pim timer

debug pim timer assert

debug pim timer assert at

debug pim timer bsr bst

debug pim timer bsr crp

debug pim timer bsr

debug pim timer hello ht

debug pim timer hello nlt

debug pim timer hello tht

debug pim timer hello

debug pim timer joinprune et

debug pim timer joinprune jt

debug pim timer joinprune kat

debug pim timer joinprune ot

debug pim timer joinprune plt

debug pim timer joinprune ppt

debug pim timer joinprune pt

debug pim timer joinprune

debug pim timer register rst

debug pim timer register

no debug pim timer

no debug pim timer assert

no debug pim timer assert at

no debug pim timer bsr bst

no debug pim timer bsr crp

no debug pim timer bsr

no debug pim timer hello ht

no debug pim timer hello nlt

no debug pim timer hello tht

no debug pim timer hello

no debug pim timer joinprune et

no debug pim timer joinprune jt

no debug pim timer joinprune kat

no debug pim timer joinprune ot

no debug pim timer joinprune plt

no debug pim timer joinprune ppt

no debug pim timer joinprune pt

no debug pim timer joinprune

no debug pim timer register rst

no debug pim timer register

Function: Enable or Disable each pim timer

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable the specified timer's debug information.

Example: Switch# debug pim timer assert

1.3.5.1.9 show ip pim bsr-router

Command: show ip pim bsr-router

Function: Display BSR address

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the BSR information maintained by the PIM.

Example: show ip pim bsr-router

PIMv2 Bootstrap information

This system is the Bootstrap Router (BSR)

BSR address: 10.1.4.3 (?)

Uptime: 00:06:07, BSR Priority: 0, Hash mask length: 10

Next bootstrap message in 00:00:00

Role: Candidate BSR

State: Elected BSR

Next Cand_RP_advertisement in 00:00:58

RP: 10.1.4.3(Vlan1)

Displayed Information	Explanations
BSR address	Bsr-router Address
Priority	Bsr-router Priority
Hash mask length	Bsr-router hash mask length
State	The current state of this candidate BSR, Elected BSR is selected BSR

1.3.5.1.10 show ip pim interface

Command: show ip pim interface

Function: Display PIM interface information

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display PIM interface information

Example: testS2(config)#show ip pim interface

Address	Interface	VIFindex	Ver/ Mode	Nbr Count	DR Prior	DR
10.1.4.3	Vlan1	0	v2/S	1	1	10.1.4.3
10.1.7.1	Vlan2	2	v2/S	0	1	10.1.7.1

Displayed Information	Explanations
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count	The interface's neighbor count
DR Prior	Dr priority
DR	The interface's DR address

1.3.5.1.11 show ip pim mroute sparse-mode

Command: show ip pim mroute sparse-mode [group <*A.B.C.D*>] [source <*A.B.C.D*>]

Function: Display the multicast route table of PIM-SM.

Parameter: group <A.B.C.D>: Display redistributed items that related to this multicast address
source <A.B.C.D>: Display redistributed items that related to this source

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the BSP routers in the network maintained by PIM-SM.

Example: Switch#show ip pim mroute sparse-mode

IP Multicast Routing Table

(*,*,RP) Entries: 0

(*,G) Entries: 1

(S,G) Entries: 0

(S,G,rpt) Entries: 0

(*, 239.192.1.10)

RP: 10.1.6.1

RPF nbr: 10.1.4.10

RPF idx: Vlan1

Upstream State: JOINED

Local

Joined

Asserted

Outgoing

Displayed Information	Explanations
Entries	The counts of each item
RP	Share tree's RP address
RPF nbr	RP direction or upneighbor of source direction.
RPF idx	RPF nbr interface
Upstream State	Upstream State,there are two state of Joined(join the tree,expect to receive data from upstream) and Not Joined(quit the tree,not expect to receive data from upstream), and more options such as RPT Not Joined, Pruned, Not Pruned are available for（S,G,rpt.）
Local	Local join interface, this interface receive IGMPJoin
Joined	PIM join interfacce, this interface receive J/P messages
Asserted	Asserted state
Outgoing	Final outgoing of multicast data, in this example,the index of the outgoing interface is 2. Command "show ip pim interface" can query interface information.

1.3.5.1.12 show ip pim neighbor

Command: show ip pim neighbor

Function: Display router neighbors

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display multicast router neighbors maintained by the PIM

Example: Switch(config)#show ip pim neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
10.1.6.1	Vlan1	00:00:10/00:01:35	v2	1 /
10.1.6.2	Vlan1	00:00:13/00:01:32	v2	1 /
10.1.4.2	Vlan3	00:00:18/00:01:30	v2	1 /
10.1.4.3	Vlan3	00:00:17/00:01:29	v2	1 /

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Neighbor interface
Uptime/Expires	Running time /overtime
Ver	Pim version ,v2 usually
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP.

1.3.5.1.13 show ip pim nexthop

Command: show ip pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the PIM buffered nexthop router information.

Example:

Switch(config)#show ip pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable

Destination Num	Type	Nexthop Addr	Nexthop Ifindex	Nexthop Name	Nexthop	Metric	Pref	Refcnt
192.168.1.1	N...	1	0.0.0.0	2006	0	0	1	
192.168.1.9	..S.	1	0.0.0.0	2006	0	0	1	

Displayed Information	Explanations
Destination	Destination of next item
Type	N: created nexthop,RP direction and S direction are not determined . R: RP derection S: source direction U: can't reach
Nexthop Num	Nexthop number
Nexthop Addr	Nexthop address
Nexthop Ifindex	Nexthop interface index
Nexthop Name	Nexthop name
Metric	Metric Metric to nexthop
Pref	Preference Route preference
Refcnt	Reference count

1.3.5.1.14 show ip pim rp-hash

Command: show ip pim rp-hash <*A.B.C.D*>

Function: Display the RP address of A,B,C,D's merge point

Parameter: Gourp address

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the RP address corresponding to the specified group address

Example: Switch(Config-if-Vlan1)#show ip pim rp-hash 239.192.1.10

RP: 10.1.6.1

Info source: 10.1.6.1, via bootstrap

Displayed Information	Explanations
RP	Queried group'sRP
Info source	The source of Bootstrap information

1.3.5.1.15 show ip pim rp mapping

Command: show ip pim rp mapping

Function: Display Group-to-RP Mapping and RP

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the current RP and mapping relationship.

Example: Switch(Config-if-Vlan1)#show ip pim rp mapping

PIM Group-to-RP Mappings

Group(s): 224.0.0.0/4

RP: 10.1.6.1

Info source: 10.1.6.1, via bootstrap, priority 6

Uptime: 00:11:04

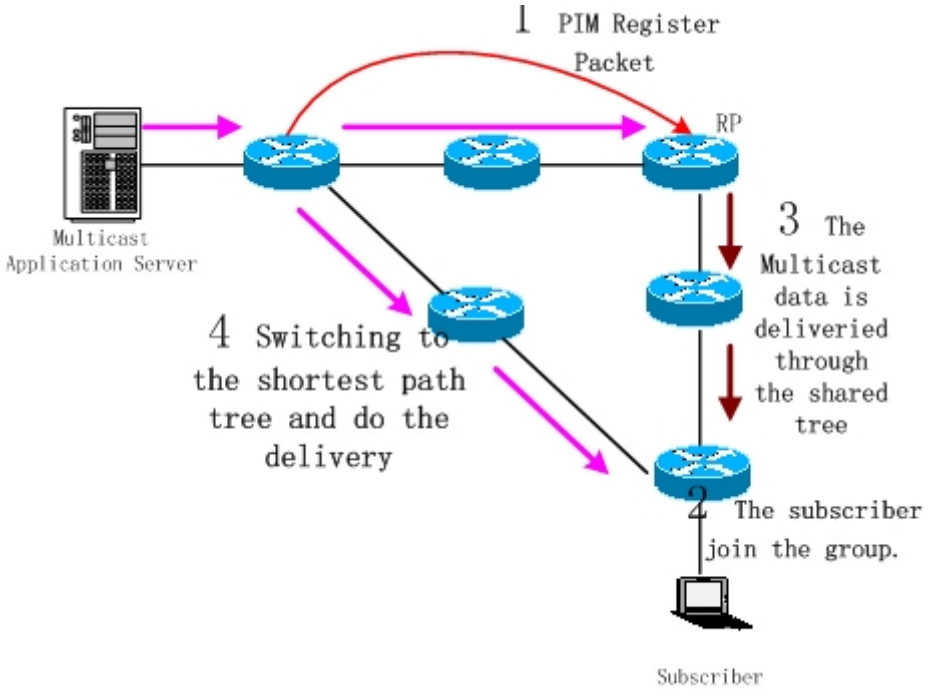
Displayed Information	Explanations
Group(s)	Group address range of RP
Info source	Source of Bootstrap messages
Priority	Priority of Bootstrap messages

1.4 MSDP

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 MSDP Configuration Task List

1. Configuration of MSDP Basic Functions

1) Enabling MSDP (Reguired)
2) Configuring MSDP entities (Reguired)
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 MSDP

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 a singe peer's cache

1. Configuration of MSDP Basic Functions

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

Prerequisites of MSDP Configurations.

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 functions, the following information should be ready.

- The IP address of MSDP entities.
- Filter policy table.

1) Enabling MSDP

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

1.Enable MSDP

2.Configure MSDP parameters

Enabling MSDP.

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

Configure MSDP parameters.

Commands	Notes
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 peers. The no form of this command will remove the configured RPF peers.
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.

2. Configuration of MSDP Entities.

Creation of MSDP Peer

Commands	Notes
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.

Configuration of MSDP parameters

Commands	Notes
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 <*nam*>**	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.

3. Configuration of Delivery of MSDP Packets.

Commands	Notes
redistribute [list <*acl-list-number* |*acl-name*>] **no redistribute**	MSDP configuration mode. To configure the filter rules for creation of SA packets.
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*>]**	MSDP configuration mode, or MSDP peer configuration mode. To configure the filter rules for receiving and forwarding SA packets. The no form of this command will remove the configured rules.
sa-request **no sa-request**	MSDP peer configuration mode. To configure sending of SA request packets. The no form of this command will disable sending of SA request packets.
sa-request-filter [list <*access-list-number* | *access-list-name*>] **no sa-request-filter [list <*access-list-number* | *access-list-name*>]**	MSDP configuration mode. 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.

4. Configuration of Parameters of SA Cache.

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

1.4.3 MSDP Configuration

1.4.3.1 cache-sa-holdtime

Command: cache-sa-holdtime <*150-3600*>

no cache-sa-holdtime

Function: To configure the longest holdtime of SA table within MSDP cache.

Parameter : <*150-3600*> : the units, range between 150 to 3600.

Command Mode: MSDP configuration Mode.

Default: 150 seconds by default.

Usage Guide: To configure the aging time of (S, G) table for MSDP cache as requirement.

Example:

Switch(config)#router msdp

Switch(router-msdp)#cache-sa-holdtime 350

1.4.3.2 cache-sa-maximum

Command: cache-sa-maximum <*sa-limit*>

no cache-sa-maximum

Function: To configure the maximum sa-limit of MSDP Peer cache specified.

Parameter: <*sa-limit*>：The maximum cache SA number，range between 1 to 75000.

Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.

Default: The maximum of cache SA number is 20000 by default.

Usage Guide: This command can be used to configure the maximum number of cached SA messages on the router in order to prevent the DoS – Deny of Service attack. The maximum number of cached SA messages can be configured in global configuration mode or in the MSDP peer configuration mode. If the configured value is less than the current number of cached SA messages, or the number configured in global mode is less than that configured in peer mode, the configuration will not function.

Example:

Switch(config)#router msdp

Switch(router-msdp)#cache-sa—maximum50000

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)#cache-sa—maximum 22000

1.4.3.3 cache-sa-state

Command: cache-sa-state

no cache-sa-state

Function: To configure the sa cache state of route.

Parameter: None.

Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.

Default: Enabled.

Usage Guide: To configure the SA cache state. If configured, the new groups will be able to get information about all the active sources from the SA cache and join the related source tree without having to wait for new SA messages. SA cache should be enabled on all the MSDP speakers. The no form of this command will remove the configuration of SA cache. To be mentioned, this command should be issued exclusively with the **sa-request** command.

Example:

Switch(config)#router msdp

Switch(router-msdp)#no cache-sa-state

1.4.3.4 clear msdp peer

Command: clear msdp peer {*peer-address*| *}

Function: Disconnected between specified MSDP Peer and TCP, to clear the statistics of the Peer.

Parameter: *peer-address*：The IP address of the Peer;

* Disconnected with all the Peer.

Command Mode: Admin Mode.

Default: None.

Usage Guide: If this command is issued with peer-address, the TCP connection to the specified MSDP peer will be removed. And all the statistics about the peer will be cleared. If no peer-address is appended, all the MSDP connections as long as relative statistics about peers will be removed.

Example:

Switch#clear msdp peer *

1.4.3.5 clear msdp sa-cache

Command: clear msdp sa-cache {group A.B.C.D|* }

Function: To clear the Source Active information in MSDP cache: the correspond data with all the source from specified group, or the correspond data with one specified (S, G) item.

Parameter: *group-address*：The IP address of multicast group，To clear group (S, G) in the Cache. *：To clear all the item in the cache.

Command Mode: Admin Mode.

Default: None.

Usage Guide: If group is specified, the non-local SA entries of the MSDP cache of the specified group will be removed. If no parameters are appended, all the non-local SA entries in the MSDP cache will be removed.

Example:

Switch#clear msdp sa-cache group 224.1.1.1

1.4.3.6 clear msdp statistics

Command: clear msdp statistics {*peer-address*| *}

Function: To clear MSDP statistic information, and not reset the session of MSDP Peer.

Parameter: None.

Command Mode: Admin Mode.

Default: None.

Example:

Switch#clear msdp statistics *

1.4.3.7 connect-source

Command: connect- source *<interface-type> <interface-number>*

no connect- source *<interface-type><interface-number>*

Function: To configure the interface address, which used for all the MSDP Peers to set up correspond connection between MSDP Peer and MSDP.

Parameter: *<interface-type> <interface-number>*：interface type and interface number.

Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.

Default: There is no specified interface by default.

Example:

Switch(config)#router msdp

Switch(router-msdp)#connect-source interface vlan 2

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)#connect-source interface loopback 10

1.4.3.8 debug msdp all

Command: debug msdp all

no debug msdp all

Function: To enable all the debugging information about MSDP.

Command Mode: Privileged configuration mode.

Default: Disabled.

Usage Guide: This command is used to enabled the debugging information of MSDP. Specific information can be selected through different triggers.

Exampe:

Switch#debug msdp all

1.4.3.9 debug msdp events

Command: debug msdp events

no debug msdp events

Function: Enable /disable the debug switch of msdp events debug.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: The event of running msdp protocol can be monitored after enable this switch.

Example:

Switch#debug msdp events

1.4.3.10 debug msdp filter

Command: debug msdp filter

no debug msdp filter

Function: Enable/disable debug switch of msdp filter policy information.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: The filter information of msdp receiving/sending message can be monitored after enable this switch.

Example:

Switch#debug msdp filter

1.4.3.11 debug msdp fsm

Command: debug msdp fsm

no debug msdp fsm

Function: Enable/disable debug switch of msdp fsm.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: Enable this switch, the fsm information of msdp peer will be displayed.

Example:

Switch#debug msdp fsm

1.4.3.12 debug msdp keepalive

Command: debug msdp keepalive

no debug msdp keepalive

Function: Enable/disable the debug switch of keepalive message information for msdp protocol.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: The information of receiving/sending keepalive message for msdp protocol can be monitored after enable this switch.

Example:

Switch#debug msdp keepalive

1.4.3.13 debug msdp nsm

Command: debug msdp nsm

no debug msdp nsm

Function: Enable/disable the debug switch of msdp nsm.

Parameter: None

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: The alternation information between running msdp protocol and nsm module can be monitored after enable this switch.

Example:

Switch#debug msdp nsm

1.4.3.14 debug msdp packet

Command: debug msdp packet {send | receive}

no debug msdp packet {send | receive}

Function: Enable/disable the debug switch of sending/receiving message for the msdp protocol.

Parameter: None

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: The receiving/sending messages of msdp protocol can be monitored after enable this switch.

Example:

Switch#debug msdp packet send

1.4.3.15 debug msdp peer

Command: debug msdp peer A.B.C.D

no debug msdp peer

Function: Enable/disable all the debug information switch of specified msdp peer.

Parameter: None

Default: Close the switch.

Command Mode: Admin Mode.

Usage Guide: Enable all the debug information of specified msdp peer as requirement, the debug information of other msdp peers will not be displayed. This command is take effect only for the specified last one msdp peer.

Example:

Switch#debug msdp peer 10.1.1.1

1.4.3.16 debug msdp timer

Command: debug msdp t**imer**

no debug msdp timer

Function: Enable/disable the debug switch of msdp timer.

Parameter: None.

Default: Close the switch.

Command Mode: Admin Mode.

Usage guide: Enable dubug information for the specified timer as requirement.

Example:

Switch#debug msdp timer

1.4.3.17 default-rpf-peer

Command: default-rpf-peer <peer-address> [rp-policy <acl-list-number>|<word>]
no default-rpf-peer

Function: To configure static RPF peer.

Parameter: <peer-address>: the IP address of the MSDP peer.
<acl-list-number>: the ACL number, only support standard ACL from 1 to 99.
<word>: the standard ACL name.

Command Mode: MSDP Configuration Mode.

Default: There is no static RPF peer by default. If the peer command only configures one MSDP peer, this peer will be treated as the default peer.

Usage Guide: To configure more than one static RPF peers, make sure to use the following two configuration methods:

Both use the rp-policy parameter: multiple RPFs take effect at the same time, and filter RP in SA messages according to the configured prefix list, and only accept SA messages allowed to pass.

Neither uses the rp-policy parameter: according to the sequence of configuration, only the first static RPF peer in the state of UP is active. All SA messages from this peer can be received while those from other peers will be dropped. If the active peer loses effect (such as the configuration is canceled or the connection is disconnected), still choose the first static RPF peer in the state of UP in the configuration sequence to be the active static RPF peer.

Example:

Switch(config)#router msdp
Switch(router-msdp)#default-rpf-peer 10.0.0.1 rp-policy 10

1.4.3.18 description

Command: description <*text*>
no description

Function: Add description information of specified MSDP Peer.

Parameter: *text:* description text, range between 1 to 80 bytes.

Command Mode: MSDP Peer Configuration Mode.

Default: There is no specified by default.

Usage Guide: To add description for the specified MSDP peer in order to identify the different MSDP configuration. The no form of this command will remove the description.

Example:

Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)#description test

1.4.3.19 exit-peer-mode

Command: exit-peer-mode

Function: Quit MSDP Peer configuration mode, and enter MSDP configuration mode.

Command Mode: MSDP Peer Configuration Mode.

Default: None.

Usage Guide: MSDP configuration mode can be returned to with the **exit-peer-mode** command, when configuration to an MSDP peer is done.

Example: Back to MSDP configuration mode from MSDP Peer configuration mode.

Switch(config-msdp-peer)# exit-peer-mode

Switch(config-msdp)#

1.4.3.20 mesh-group

Command: mesh-group <*name*>

no mesh-group <*name*>

Function: To configure MSDP peer as specified mesh group number, if set the same MSDP peer to many mesh groups, then the last mesh group is available.

Parameter: name：Mesh-group name.

Command Mode: MSDP Peer Configuration Mode.Default: MSDP peer doesn't belong to any mesh group by default.

Usage Guide: Mesh group can reduce SA message flooding and predigest Peer-RPF checking.

Example:

Switch(config)#router msdp

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)#mesh-group test

1.4.3.21 originating-rp

Command: originating-rp <*interface-type*> <*interface-number*>

no originating-rp

Function: To configure the IP address of the specified interface as the IP address of the RP in the SA messages.

Parameter: <*interface-type*> <*interface-number*>: interface-type and interface-number.

Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.

Default: The default RP address of SA message is the RP address of PIM configured.

Usage Guide: To configure the IP address of the specified interface as the IP address of the RP in the SA messages. If no IP address is configured for the specified interface, or the interface is down, no SA messages will be advertised. In this occasion, if multiple RP is configured for the device, other SA messages for other RP will not be advertised either. Hence, it is required that

the interface should be working when being configured.

Example:

Switch(config)#router msdp

Switch(router-msdp)#originating-rp vlan 20

1.4.3.22 peer

Command: peer <*A.B.C.D*>

no peer <*A.B.C.D*>

Function: To configure MSDP peer, enter MSDP Peer mode; The no form command delete the configured MSDP Peer.

Command Mode: MSDP Configuration Mode.

Default: There is no MSDP Peer be configured by default.

Usage Guide: To configure the IP address of the MSDP peer, and enter the peer configuration mode. When the command is issued, the router will setup the TCP session to the specified peer. The no form of this command will remove the configured MSDP peer, and destroy all the sessions and related statistics with the specified peer.

Example: To configure MSDP Peer in MSDP congfiguration mode.

Switch(config-msdp)#peer 10.1.1.1

Switch(config-msdp-peer)#

1.4.3.23 redistribute

Command: redistribute [list <*acl-list-number* | *acl-name*>]

no redistribute

Function: To configure the redistribute of SA messages.

Parameter: *acl-number*：*acl-number*：specified advanced ACL number（100-199）。

acl-name：specified ACL name.

Command Mode: MSDP Configuration Mode.

Default: When set up SA message, announce all the source within fired, but not confine the (S, G) item.

Usage Guide: If ACL list number is specified, only the (S, G) entries which have passed the ACL check will be advertised in the SA messages. If no ACL is specified, no (S, G) entry will be advertised in the SA messages.

Example:

Switch(config)#router msdp

Switch(router-msdp)# redistribute list 130

1.4.3.24 remote-as

Command: remote-as <*as-num*>

no remote-as <*as-num*>

Function: To configure AS number of specified MSDP Peer.

Parameter: *as -num*：AS number，range between 1 to 65535.

Command Mode: MSDP Peer Configuration Mode.Default: The AS number isn't initialized to 0 by default.

Usage Guide: This command specifies the AS number manually.

Example:

Switch(config)#router msdp

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)#remote-as 20

1.4.3.25 router msdp

Command: router msdp

no router msdp

Function: Enable the msdp protocol of the switch, enter MSDP mode; the no form command disable MSDP protocol.

Command Mode: Global Mode.

Default: Disabled.Usage Guide: Enable MSDP on global mode, but even configured PIM SM at the same time , then the MSDP can be work.

Example: Enable MSDP on global mode.

Switch(config)#router msdp

1.4.3.26 sa-filter {in | out}

Command: 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*>]

Function: To configure the filter policy of receiving or transmitting messages, which can be used to control the receiving and transmitting source message.

Parameter: in: To filter the SA messages from specified MSDP Peer.

out： To filter the SA messages transmitted from specified MSDP Peer.

acl-number：Specified advanced ACL number（100-199）。

acl-name：Specified advanced ACL name.

rp-acl-number：Specified standard ACL number（1-99）。

rp-*acl-name*：Specified standard ACL name. If the parameter isn't specified, all the SA message which include (S, G) item will be filtered.

Command Mode: MSDP Configuration Mode and MSDP Peer Configuration Mode.

Default: All the SA messages receiving or transmitting will not be filtered.

Usage Guide: Configuration in the peer mode will override that in the MSDP configuration mode. The distribution of SA messages can be controlled through this command or the redistribute command.

Example:

Switch(config)#router msdp

Switch(router-msdp)# sa-filter in

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)# sa-filter in list 120

1.4.3.27 sa-request

Command: sa-request

no sa-request

Function: To configure the route sending SA request message to specified MSDP Peer when received the joined message from a new group.

Parameter: None.

Command Mode: MSDP Peer Configuration Mode.

Default: Not sending SA Request message by default.

Usage Guide: This command makes the switch (RP) send SA request messages to the specified MSDP. When there is a new group or member, the switch (RP) will send SA request messages to the specified MSDP and wait for the latter's response of its cached local SA messages. After sending a SA message to the specified MSDP, RP will receive a SA_response message from the peer, and know all active sources of the peer (not including the source information learnt via MSDP SA). If RP is configured with SA cache state, this configuration won't take effect. This command is mutually exclusive to sa-cache-sate. If the MSDP is configured with SA cache state, it won't be able to configure sa-request. The switch will show a prompt to notice the users. Please notice this command only applies to RP.

Example:

Switch(config)#router msdp

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)#sa-request

1.4.3.28 sa-request-filter

Command: sa-request-filter [list <*access-list-number* | *access-list-name*>]

no sa-request-filter [list <*access-list-number* | *access-list-name*>]

Function: All the SA request message from MSDP Peer will be filtered.

Parameter: *access-list-number*：ACL number, only supported standard ACL from 1 to 99.

access-list-name：ACL name

Command Mode: MSDP Configuration Mode.

Default: The route receives all the SA request message from MSDP Peer.

Usage Guide: If no list parameter is specified, all the SA request messages from MSDP peers will be filtered. If specified, SA request messages will be filtered with the specified ACL list.

Example:

Switch(config)#router msdp

Switch(router-msdp)#sa-request-filter list 1

1.4.3.29 show msdp global

Command: show msdp global

Command Mode: Under all the views.

Usage Guide: Show the configuration information in MSDP mode, include the state of MSDP protocol, Cache and so on.

Example:

Switch#show msdp global

Multicast Source Discovery Protocol (MSDP):

SA-Cached, Originator: Vlan2, Connect-Source: Vlan2

MAX External SA Entry: 200000

MAX Peer External SA Entry: 20000

TTL Threshold: 0

SA Entry Hold Time: 350

Filters:

Redistribute_filter: Not set

SA-filter:

[IN]: RP-list: None, SG-list: None

[OUT]:Not Configured

SA-Request-Filter: Not Configured

Default Peer:

Not Configured

Mesh Group:

The introduction of showed items：

Field	**Notes**
SA-Cached	MSDP SA-Cached state
Originator	The RP interface of MSDP originated.
MAX External SA Entry	The max entries configured in MSDP configuration mode.
MAX Peer External SA Entry	The max entries of each Peer.

TTL Threshold	TTL Threshold
SA Entry Hold Time	The multicast source hold time of MSDP cache.
Redistribute_filter	To establish the filter policy of SA message.
SA-filter [IN | OUT]	The filter policy of receiving or sending SA message.
Default Peer	static RPF Peer
Mesh Group	The name and members of mesh group.

1.4.3.30 show msdp local-sa-cache

Command: show msdp local-sa-cache

Function: Display the information for local-sa-cache.

Parameter: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guide: Display the information for local-sa-cache.

Example:

Switch#show msdp local-sa-cache

MSDP Flags:

E - set MRIB E flag, L - domain local source is active,

EA - externally active source, PI - PIM is interested in the group,

DE - SAs have been denied.

Cache SA Entry:

Source Address	Group Address	RP Address	TTL
5.5.5.9	225.0.0.1	11.1.1.1	64
5.5.5.9	225.0.0.2	11.1.1.1	64
5.5.5.9	225.0.0.3	11.1.1.1	64
5.5.5.9	225.0.0.4	11.1.1.1	64

1.4.3.31 show msdp peer

Command: show msdp peer <A.B.C.D>

Parameter:

Command Mode: Under all the views.

Usage Guide: Show the configuration information in MSDP configuration mode.

Example:

Switch#show msdp peer 31.1.1.3

MSDP Peer 31.1.1.3 , AS 0 , Description:
Connection status:
State: Established, Resets: 0,
Connection Source: Not set , Connect address: 31.1.1.1
Uptime(Downtime): 00h:07m:53s, SA messages received:16
TLV messages sent/received: 8 /24
SA messages incoming Rejected: 0
SA messages outgoing Rejected: 0
SA Filtering:
Input filter Not Configured
Output filter Not Configured
SA-Requests:
Input filter Not Configured
Sending SA-Requests to peer: Disabled
Peer ttl threshold: 0

The introduction of showed items：

Field	**Notes**
MSDP Peer	IP address of MSDP Peer
State	MSDP Peer state
Connection source	The interface used in local TCP connection
Uptime(Downtime)	The uptime or downtime of MSDP peer.
TLV Messages sent/received	The statistics of messages sent and received from the Peer.
SA Filtering	The filtering policy configured with Peers.
SA-Requests	The configured filtering policy of SA requests.

1.4.3.32 show msdp sa-cache

Command: show msdp sa-cache { <*source-address*> [<*group-address*>] | as-num <*sas-number*> | peer <*peer-address*>| rpaddr <*rp-address*>}
Function: Display the configuration information for cache-exterior source under MSDP.
Parameter: *source-address*：source address.
group-address：group address.
as-number：*autonomous-system-number* autonomous system number.
peer-address：Peer address.
rp-address：RP address.

Command Mode: Under all the views.

Usage Guide: Show the configuration information for cache-exterior source under MSDP.

Example:

Switch#show msdp sa-cache 30.30.30.1

MSDP Flags:

E - set MRIB E flag, L - domain local source is active,

EA - externally active source, PI - PIM is interested in the group,

DE - SAs have been denied.

Cache SA Entry:

(S:30.30.30.1, G: 224.1.1.1, RP: 10.1.1.2), AS: 0, 00h:00m:11s/00h:02m:19s

Learn From Peer:20.1.1.1, RPF Peer: 10.1.1.10

SA Received: 10 Encapsulated data received: 0

grp flags: None source flags: EA, DE

The explanation of showed items:

field	**Notes**
(S，G，RP)	running source message information(S，G，RP)
AS Num	autonomous system number
update time	SA message cache time
expire time	SA message expire time
Learn From Peer	The table is learned from the Peer
RPF Peer	RPF Peer of the entry
SA Received	SA message which include the entry.
Encapsulated data received	The multicast message encapsulated in SA message.
grp flags	The multicast group flag in the entry.
source flags	The multicast source flag in the entry.

1.4.3.33 show msdp sa-cache summary

Command: show msdp sa-cache summary

Command Mode: Under all the views

Usage Guide: Show the summary of MSDP Cache.

Example:

Switch#show msdp sa-cache summary

MSDP Flags:

E - set MRIB E flag, L - domain local source is active,

EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.

Cache SA Entry:
Total number of SA Entries = 1
Total number of Sources = 1
Total number of Groups = 1
Total number of RPs = 1

Originator-RP	SA total	RPF peer
10.1.1.2	1	10.1.1.10

AS-num	SA total
0	1

The introduction of showed items:

Field	**Notes**
Total number of SA Entries	Total number of SA entries in the cache.
Total number of Sources	Total number of different multicast sources in the cache.
Total number of Groups	Total number of different multicast groups in the cache.
Total number of RPs	Total number of different RP in the cache.
Originator-RP	Originated RP address.
SA total	Total number of received SA message from RP.
RPF peer	The RPF Peer address of corresponding RP.
AS-num	Autonomous system number.

1.4.3.34 show msdp statistics

Command:show msdp statistics peer [*Peer-address*]
Function: Show the statistics of messages from specified Peer.
Parameter: *Peer-address*： Show the statistics of messages from specified Peer.
Command Mode: Under all the views.
Usage Guide: Show all the statistics of specified Peer or receiving/sending messages from all the Peers.
Example:

Switch#show msdp sta peer 2.2.2.4

MSDP Peer Statistics :

Peer 2.2.2.4 , AS is 0 , State is Inactive

TLV Rcvd : 76 total

39 keepalives, 37 SAs

0 SA Requests, 0 SA responses

TLV Send : 80 total

41 keepalives, 39 SAs

0 SA Requests, 0 SA responses

SA msgs : 37 received, 39 sent

Field	**Notes**
Peer	MSDP Peer address
AS	Autonomous system number
State	MSDP Peer state
TLV Rcvd	The TLV type and statistics of Peer received.
TLV Send	The TLV type and statistics of Peer sent
SA msgs	The SA message statistics of Peer received and send.

1.4.3.35 show msdp summary

Command: show msdp summary

Command Mode: Under all the views.

Usage Guide: Show the summary of MSDP.

Example:

Switch#show msdp summary

Maximum External SA's Global : 20000

MSDP Peer Status Summary

Peer Address AS State Uptime/ Reset Peer Active Cfg.Max TLV
Downtime Count Name SA Cnt Ext.SAs recv/sent

2.2.2.4 0 Established THU JAN 01 00:00:00 10 0 121/100

The introduction of showed items:**Field**	**Notes**
Peer Address	IP address of MSDP Peer

AS	Autonomous system number belonged toMSDP Peer
State	MSDP Peer state
Uptime/Downtime	The uptime or downtime of MSDP peer.
Reset Count	The reset count of MSDP Peer.
Peer Name	The description of MSDP Peer.
Active SA	The numbers of active SA
TLV sent/received	The statistics of TLV messages sent and received from the Peer.

1.4.3.36 shutdown

Command: shutdown

no shutdown

Function: Disable specified MSDP Peer.

Parameter: None.

Command Mode: MSDP Peer Configuration Mode.

Default: Enabled.

Usage Guide: When configuring a MSDP peer with multiple commands, sometimes it is required that the these commands should be effect together but not one by one. The **shutdown** command can be used to disable the peer before configuration and the no shutdown used after configuration in order to make the peer configuration effect together. The shutdown command will remove all the TCP sessions with the specified MSDP peer as well as the statistics.

Example:

Switch(config)#router msdp

Switch(router-msdp)#peer 20.1.1.1

Switch(router-msdp-peer)#shutdown

1.4.3.37 ttl-threshold

Command: ttl-threshold *<ttl>*

no ttl-threshold

Function: To configure the minimum TTL value of multicast source encapsulated in SA message.

Parameter: *ttl*：minimum TTL value，range between 1 to 255.

Command Mode: MSDP Configuration Mode.

Default: TTL value will not be filtered when TTL value is 0.

Usage Guide: The redistribution of multicast datagrams can be controlled through the TTL value.

SA messages will be advertised only if the TTL value in the packet is less than the TTL threshold.

Example:

Switch(config)#router msdp

Switch(router-msdp)#ttl-threshold 10

1.4.4 MSDP Configuration Example:

Example1: MSDP basic functions

Multicast Routing Configuration:

1. Suppose the multicast server is sending multicast datagrams at 224.1.1.1.
2. The designated router – DR, which is connected to the multicast server, encapsulate the multicast datagrams in the Register packets and send them to the RP in the local domain.
3. The RP unwraps the 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 datagrams 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.
6. 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.When the reverse route has been set up, the multicast datagrams from the source will be directly delivered to RP3, and RP will forward the datagrams 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.

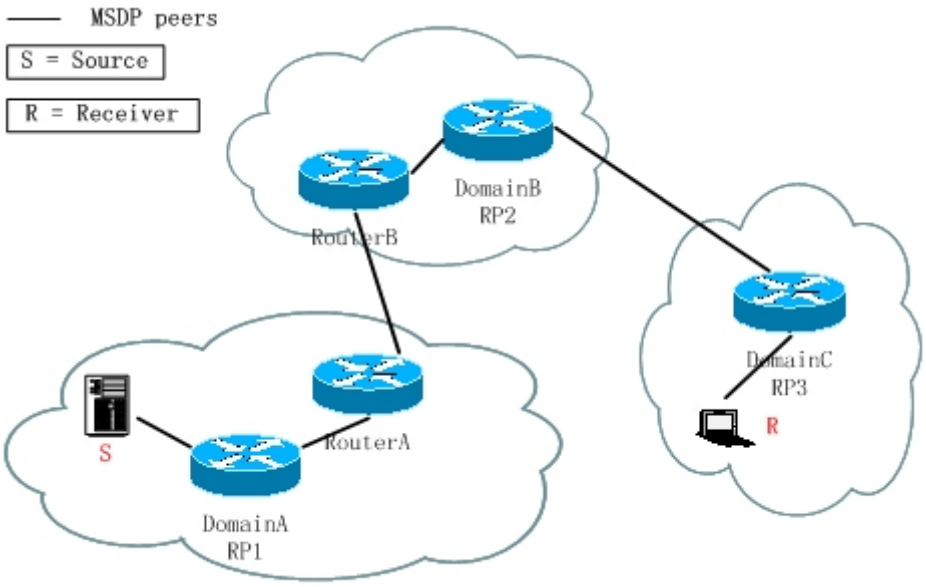


Fig 1-3 Network Topology for MSDP Entries.

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, when mesh group is configured for the four meshed peers in the same domain, flooding of SA messages reduced remarkably

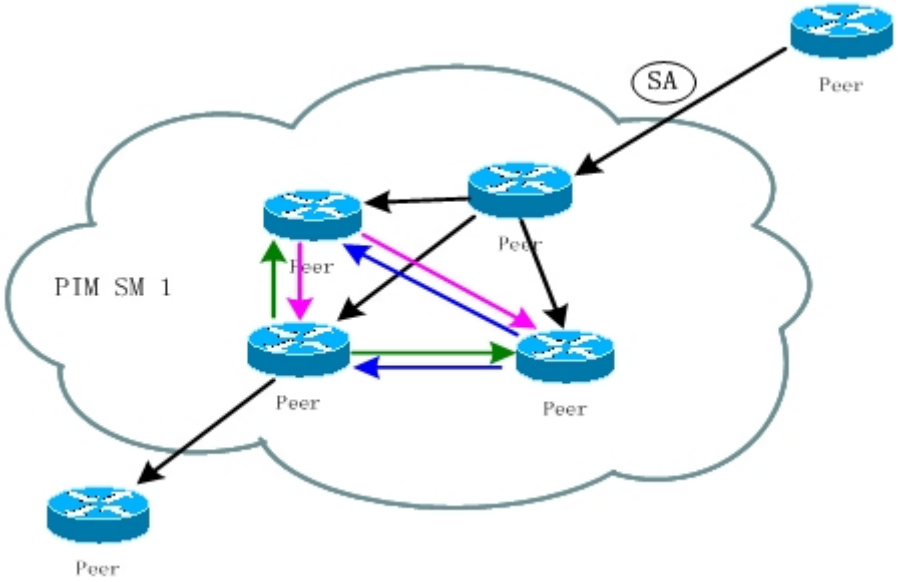


Fig 1-4 Flooding of SA messages

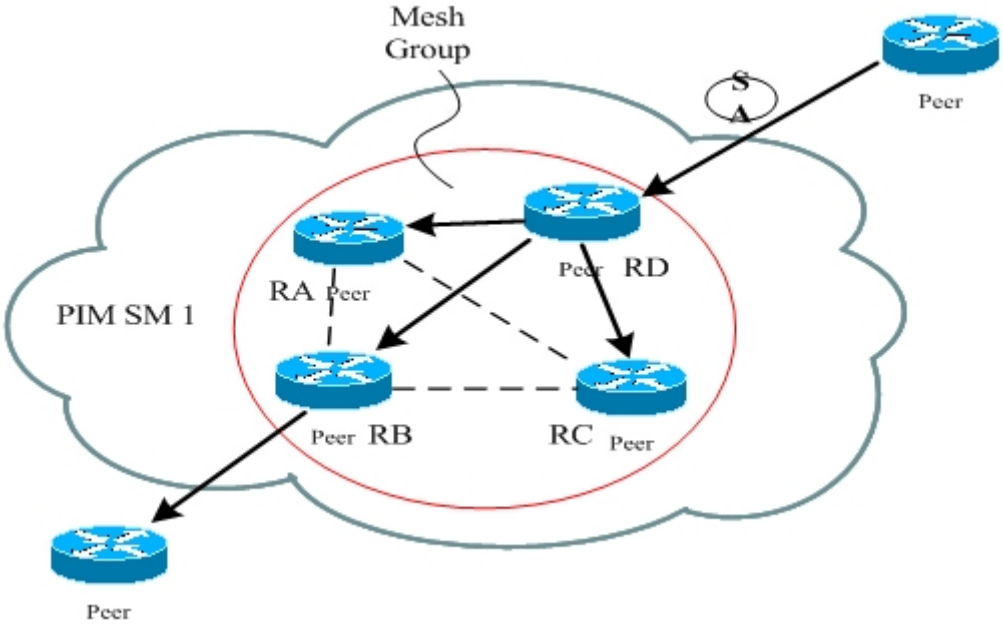


Fig 1-5 Flooding of SA messages with mesh group configuration

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
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 20.1.1.4
Switch(router-msdp)#mesh-group test
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 30.1.1.3
Switch(router-msdp)#mesh-group test
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
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 40.1.1.4
Switch(router-msdp)#mesh-group test
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 60.1.1.3

Switch (router-msdp)#mesh-group test

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
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 40.1.1.4
Switch(router-msdp)#mesh-group test
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 60.1.1.2
Switch(router-msdp)#mesh-group test

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
Switch(msdp-peer)#exit

Switch(router-msdp)#peer 40.1.1.2
Switch(router-msdp)#mesh-group test
Switch(msdp-peer)#exit
Switch(router-msdp)#peer 50.1.1.3
Switch(router-msdp)#mesh-group test

1.4.5 MSDP Trouble Shooting

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 Digital China Network Support Center for support.

1.5 ANYCAST RPv4 Configuration

1.5.1 ANYCAST RPv4 Introduction

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 RPs will cause a new problem that is if the multicast source and the receivers are registered to different RPs, 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 RPs, Anycast RP defines that the nearest RP to the multicast source should forward the source register messages to all the other RPs to guarantee that all joiners of the RPs 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 RPv4 Configuration Task

1. Enable ANYCAST RPv4 function
2. Configure ANYCAST RPv4

1. Enable ANYCAST RPv4 function

Command	Explanation
Global configuration mode	
ip pim anycast-rp **no ip pim anycast-rp**	Enable ANYCAST RP function. (In order to actually enable the ANYCAST RP protocol, the following command is needed)(necessary). No operation will globally disable ANYCAST RP function.

2. Configure ANYCAST RPv4

(1) Configure the RP candidate

Command	Explanation
Global configuration mode	
ip pim rp-candidate {vlan<*vlan-id*> | loopback<*index*> |	Now, the PIM-SM has allowed the Loopback interface to be a RP

***<ifname>*} [<*A.B.C.D*>] [<*priority*>]** **no ip 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 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 RPs. 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 RPs 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.

(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 RPs 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 the other-rp-addresses of other RPs communicating with it. This unicast address identifies other RPs and is used in the communication with local routers. The effect of **other-rp-address** refers to 2 respects: 1. Once this router (as a RP) receives the register message from a DR unicast, it should forward it to other RPs in the

	network to notify all the RPs 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 RPs one by one. No operation will cancel an other-rp-address communicating with this router.

1.5.3 ANYCAST RPv4 Configuration Commands

1.5.3.1 debug pim anycast-rp

Command：debug pim anycast-rp

no debug pim anycast-rp

Function：Enable the debug switch of ANYCAST RP function; the no operation of this command will disable this debug switch.

Command Mode：Admin mode.

Default：The debug switch of ANYCAST RP is disabled by default.

Usage Guide：This command is used to enable the debug switch of ANYCAST RP of the router, it can display the information of handling PIM register packet of the switch——packet, and the information of events——event.

Example：

Switch#debug pim anycast-rp

1.5.3.2 ip pim anycast-rp

Command：ip pim anycast-rp

no ip pim anycast-rp

Function：Enable the ANYCAST RP of the switch; the no operation of this command is to disable the ANYCAST RP function.

Command Mode：Global configuration mode.

Default：The switch will not enable the ANYCAST RP by default.

Usage Guide：This command will globally enable ANYCAST RP protocol, but, in order to make ANYCAST RP work, it is necessary to configure self-rp-address and other-rp-address set.

Example：Enable ANYCAST RP in global configuration mode.

Switch(config)#ip pim anycast-rp

1.5.3.3 ip pim anycast-rp

Command：**ip pim anycast-rp <*anycast-rp-addr*> <*other-rp-addr*>**

no ip pim anycast-rp <*anycast-rp-addr*> <*other-rp-addr*>

Function：Configure ANYCAST RP address（ARA）and the unicast addresses of other RPs communicating with this router(as a RP). The no operation of this command will cancel the unicast address of another RP in accordance with the configured RP address.

Parameters：***anycast-rp-addr***：RP address, the absence of the candidate interface in accordance with the address is allowed.

other-rp-addr：the unicast address of other RP communicating with this router(as a RP).

Command Mode: Global configuration mode.

Default：There is no configuration by default.

Usage Guide：

1 The anycast-rp-addr configured on this router(as a RP) is actually the RP address configured on multiple RPs in the network, in accordance with the address of RP candidate interface (or Loopback interface). The current absence of the candidate interface in accordance with the address is allowed when configuring.

2 Configure the other-rp-address of other RPs communicating with this router(as a RP). The unicast address identifies other RPs, and is used to communicate with the local router.

3 Once this router (as a RP) receives the register message from a DR unicast, it should forward it to other RPs in the network to notify all the RPs 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.

4 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 RPs one by one.

Example：Configure other-rp-address in global configuration mode.

Switch(config)#ip pim anycast-rp 1.1.1.1 192.168.3.2

1.5.3.4 ip pim anycast-rp self-rp-address

Command：**ip pim anycast-rp self-rp-address <*self-rp-addr*>**

no ip pim anycast-rp self-rp-address

Function：Configure the self-rp-address of this router(as a RP). This address will be used to

exclusively identify this router from other RPs, and to communicate with other RPs. The no operation of this command will cancel the configured unicast address used by this router (as a RP) to communicate with other RPs.

Parameters：*self-rp-addr*：the unicast address used by this router (as a RP) to communicate with other RPs.

Command Mode：Global configuration mode.

Default：No self-rp-address is configured by default.

Usage Guide：

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 RPs 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.

3 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.

Example：Configure the self-rp-address of this router in global configuration mode.

Switch(config)#ip pim anycast-rp self-rp-address 1.1.1.1

1.5.3.5 ip pim rp-candidate

Command：ip pim rp-candidate {vlan<*vlan-id*> | loopback<*index*> | <*ifname*>} [<*A.B.C.D*>] [<*priority*>]

no ip pim rp-candidate

Function：Add a Loopback interface as a RP candidate interface based on the original PIM-SM command; the no operation of this command is to cancel the Loopback interface as a RP candidate interface.

Parameters：*index*：Loopback interface index, whose range is <1-1024>.

***vlan-id*:** the Vlan ID.

***ifname*:** the specified name of the interface.

A.B.C.D/M: the ip prefix and mask.

***<priority>*:** the priority of RP election, ranging from 0 to 255, the default value is 192. The smaller the value is the higher the priority is.

Command Mode：Global configuration mode.

Default Setting：No RP interface is configured by default.

Usage Guide：In order to support ANYCAST RP function, new rule allows configuring a Loopback interface to be the RP candidate interface. The RP candidate interface should be

currently unique, and the address of which should be added into the router to make sure that PIM router can find the nearest RP. The “no ip pim rp-candidate” command can be used to cancel the RP candidate.

Example： Configure Loopback1 interface as the RP candidate interface in global configuration mode.

Switch(config)#ip pim rp-candidate loopback1

1.5.3.6 show debugging pim

Command：show debugging pim

Command Mode： Admin mode

Usage Guide： The current state of anycast rp debug switch.

Example：

Switch(config)#show debugging pim

Debugging status:

PIM anycast-rp debugging is on

1.5.3.7 show ip pim anycast-rp first-hop

Command：show ip pim anycast-rp first-hop

Command Mode： Admin mode

Usage Guide： Display the state information of anycast rp, and display the mrt node information generated in the first hop RP which is currently maintained by the protocol.

Example：

Switch(config)#show ip pim anycast-rp first-hop

IP Multicast Routing Table

(*,G) Entries: 0

(S,G) Entries: 1

(E,G) Entries: 0

INCLUDE (192.168.1.136, 224.1.1.1)

Local .l.....

Display	Explanation
Entries	The number of all kinds of entries
INCLUDE	The information of mrt generated in the first hop RP

1.5.3.8 show ip pim anycast-rp non-first-hop

Command：show ip pim anycast-rp non-first-hop

Command Mode： Admin mode

Usage Guide： Display the state information of anycast rp, and display the mrt node information generated in the non first hop RP which is currently maintained by the protocol, that is the mrt node information which is created after the first hop RP transfers the register message it received to this RP.

Example：

Switch(config)#show ip pim anycast-rp non-first-hop

IP Multicast Routing Table

(*,G) Entries: 0

(S,G) Entries: 1

(E,G) Entries: 0

INCLUDE (192.168.10.120, 225.1.1.1)

Local .l.....

Display	Explanation
Entries	The number of all kinds of entries
INCLUDE	The mrt information created in the first hop RP.

1.5.3.9 show ip pim anycast-rp status

Command：show ip pim anycast-rp status

Command Mode： Admin mode

Usage Guide： Display the configuration information of ANYCAST RP, whether ANYCAST RP globally enables, whether the self-rp-address is configured and the list of currently configured anycast rp set.

Example：

Switch(config)#show ip pim anycast-rp status

Anycast RP status:

anycast-rp:Enabled!

self-rp-address:192.168.3.2

anycast-rp address: 1.1.1.1

other rp unicast rp address: 192.168.2.1

other rp unicast rp address: 192.168.5.1

anycast-rp address: 192.168.1.4

other rp unicast rp address: 192.168.2.1

Display	Explanation
anycast-rp:	Whether the anycast rp switch is globally enabled
self-rp-address:	The configured self-rp-address
anycast-rp address:	The configured anycast-rp-address
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address
anycast-rp address:	The configured anycast-rp-address*
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address

1.5.4 ANYCAST RPv4 Configuration Examples

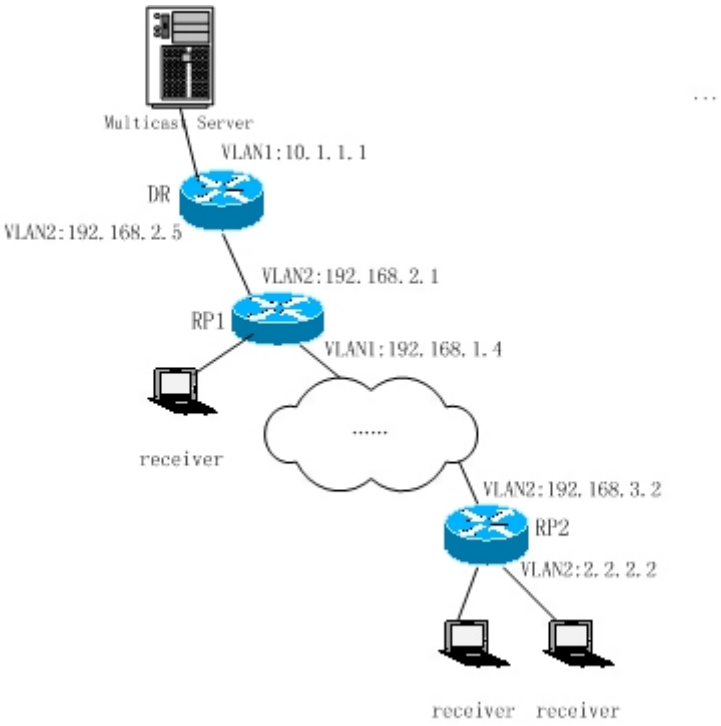


Fig 1-6 The ANYCAST RP v4 function of the router

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 RPs 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

1.5.5 ANYCAST RPv4 Troubleshooting Help

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;
- ✧ 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 pim anycast-rp” or “debug ipv6 pim anycast-rp”, then copy the DEBUG information within 3 minutes and send it to the technology service center.

1.6 DVMRP

1.6.1 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 treat 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 (ues 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 makes use of 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 arrivable, 33 to 63 means the switch which generates the report message will receive multicast packets from specific source depending on upstream router.

1.6.2 Configuration Task List

1、Globally enable and disable DVMRP (required)

2、Configure Enable and Disable DVMRP Protocol at the interface (optional)

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 EDGECORE series 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)

1. Enable DVMRP Protocol on the interface

The basic configuration to function DVMRP routing protocol on EDGECORE series 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.

1.6.3 Command For DVMRP

1.6.3.1 ip dvmrp

Command: ip dvmrp

no ip dvmrp

Function: Configure to enable DVMRP protocol on interface; the "**no ip dvmrp**" command disenables DVMRP protocol.

Parameter: None

Default: Disable DVMRP Protocol

Command Mode: Interface Configuration Mode

Usage Guide: The interface processes DVMRP protocol messages, only excuting DVMRP protocol on interface.

Example: Enable DVMRP Protocol on interface vlan1.

Switch (config)#interface vlan 1

Switch(Config-If-vlan1)#ip dvmrp

1.6.3.2 ip dvmrp metric

Command: ip dvmrp metric <*metric_val*>

no ip dvmrp metric

Function: Configure interface DVMRP report message metric value; the "**no ip dvmrp metric**" command restores default value.

Parameter: <*metric_val*> is metirc value, value range from 1 to 31

Default: Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: The routing information in DVMRP report messages includes a groupsource network and metric list. After configuring interface DVMRP report message metric value, it makes all received routing entriy from the interface adding configured interface metric value as new metric value of the routing. The metric value applies to calculate posion reverse, namely ensuring up-downstream relations. If the metric value of some route on the switch is not less than 32, it explains the route can be reach. If it is downstream of some route after calculation and judgement, it will transmit report message included the route to upstream. The route metric increases 32 based on original value in order to indicate downstream itself.

Example: Configure interface DVMRP report message metric value: 2

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip dvmrp metric 2

1.6.3.3 ip dvmrp multicast-routing

Command: ip dvmrp multicast-routing

no ip dvmrp multicast-routing

Function: Globally enable DVMRP protocol; the "no ip dvmrp multicast-routing" command globally disenables DVMRP protocol

Parameter: None

Default: Defalut

Command Mode: Global Mode

Usage Guide: Dvmrp multicast-protocol can enable after globally execute the command

Example: Switch (config)#ip dvmrp multicast-routing

1.6.3.4 ip dvmrp output-report-delay

Command: ip dvmrp output-report-delay <*delay_val*> [<*burst_size*>]

no ip dvmrp output-report-delay

Function: Configure the delay of DVMRP report message transmitted on interface and transmitted message quantity every time, the "**no ip dvmrp output-report-delay**" command restores default value.

Parameter: <*delay_val*> is the delay of periodically transmitted DVMRP report message, value range from 1s to 5s.

<*burst_size*> is a quantity of transmitted message every time, value range from 1 to 65535

Default: Default the delay of transmitted DVMRP report message as 1s, default: transmitting two messages every time.

Command Mode: Interface Configuration Mode

Usage Guide: Avoid message burst if setting an appropriate delay.

Example: Switch (Config-If-vlan1)#ip dvmrp output-report-delay 1 1024

1.6.3.5 ip dvmrp reject-non-pruners

Command: ip dvmrp reject-non-pruners

no ip dvmrp reject-non-pruners

Function: Configure to reject neighborship with DVMRP router of non pruning/grafting on the interface, the "**no ip dvmrp reject-non-pruners**" command restores neighborship can be established.

Parameter: None

Default: Default

Command Mode: Interface Configuration Mode

Usage Guide: The command determines if it will establish neighboringship with DVMRP router of non pruning/grafting or not.

Example: Switch (Config-If-vlan1)#ip dvmrp reject-non-pruners

1.6.3.6 ip dvmrp tunnel

Command: ip dvmrp tunnel <*index*> <*src-ip*> <*dst-ip*>

no ip dvmrp tunnel {***<index>*** **|*<src-ip>* *<dst-ip>*}**

Function: Configure a DVMRP tunnel; the "**no ip dvmrp tunnel** {***<index>*** **|*<src-ip>* *<dst-ip>*}**" command deletes a DVMRP tunnel.

Parameter: ***<src-ip>*** is source IP address,

<dst-ip> is remote neighbor IP address,

<index> is tunnel index number, value range from 1 to 65535.

Default: Default: Do not Configure DVMRP tunnel.

Command Mode: Global Mode

Usage Guide: Because not all of switches support multicast, DVMRP supports tunnel multicast communication. The tunnel is a way of transmitted multicast data packet among DVMRP switches partitioned off switches without supporting multicast routing. It acts as a virtual network between two DVMRP switches. Multicast data packages packed in unicast data packages, directly are transmitted to next supporting multicast switch. DVMRP protocol equally deal with tunnel interface and general physical interface. After configuring no ip dv multicast-routing, all of the tunnel configurations are deleted.

Example: Switch(config)#ip dvmrp tunnel 1 12.1.1.1 24.1.1.1

1.6.4 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.

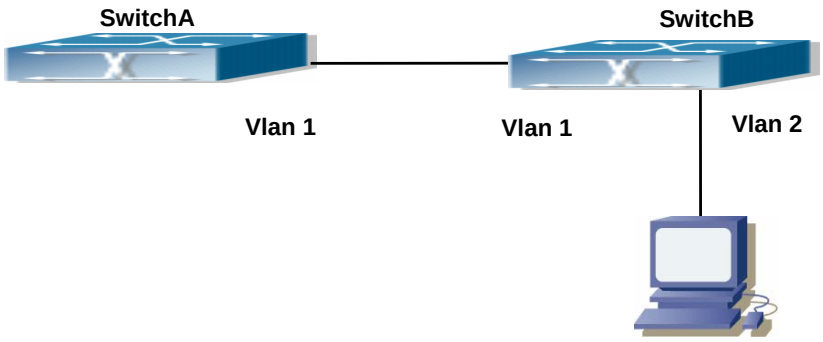


Fig 1-7 DVMRP Network Topology Diagram

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

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 dvmrp
(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
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.

1.6.5 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.

1.6.5.1 Monitor And Debug Command

1.6.5.1.1 debug dvmrp

Command: debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] |route]|

nsm|mfc|mib|timer [probe[probe-timer|neighbor-expiry-timer]| prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]|route[report-timer|flash-upd-timer|route-expiry-timer|route-holdown-timer|route-burst-timer]]|packet[[probe [in|out] | report [in|out | prune [in|out] graft [in|out] | graft-ack [in|out] |in|out]]|all]

no debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] |route]|nsm|mfc|mib|timer[probe[probe-timer|neighbor-expiry-timer]|prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]|route[report-timer|flash-upd-timer|route-expiry-timer|route-holdown-timer|route-burst-timer]]|packet[[probe [in|out] | report [in|out | prune [in|out] graft [in|out] | graft-ack [in|out] |in|out]]|all]

Function: Display DVMRP protocol debugging message; the "**no debug dvmrp [events[neighbor|packet|igmp|kernel|prune [detail] |route]| nsm| mfc|mib|timer [probe[probe-timer|neighbor-expiry-timer]| prune[prune-expiry-timer|prune-retx-timer|graft-retx-timer]| route[report-timer|flash-upd-timer|route-expiry-timer| route-holdown-timer|route-burst-timer]] |packet[[probe [in|out] | report [in|out | prune [in|out] graft [in|out] | graft-ack [in|out] |in|out]]|all]**" command disenables this debugging switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable this switch, and display DVMRP protocol executed relevant messages.

1.6.5.1.2 show ip dvmrp

Command: show ip dvmrp

Function: Display DVMRP protocol information.

Parameter: None

Default: Do not display (Off)

Command Mode: Any Configuration Mode

Usage Guide: The command applies to display some total statistic information of DVMRP protocol

Example:

Switch#show ip dvmrp

DVMRP Daemon Start Time: MON JAN 01 00:00:09 2001

DVMRP Daemon Uptime: 17:37:03

DVMRP Number of Route Entries: 2

DVMRP Number of Reachable Route Entries: 2

DVMRP Number of Prune Entries: 1

DVMRP Route Report Timer: Running

DVMRP Route Report Timer Last Update: 00:00:56

DVMRP Route Report Timer Next Update: 00:00:04

DVMRP Flash Route Update Timer: Not Running

1.6.5.1.3 show ip dvmrp interface

Command: show ip dvmrp interface [<*ifname*>]

Function: Display DVMRP interface

Parameter: <*ifname*> is interface name, namely displaying configured interface information of specified interface.

Default: Do not display (Off)

Command Mode: Any Configuration Mode

Example: Switch #show ip dvmrp in vlan4

Address	Interface	Vif Index	Ver.	Nbr Cnt	Type	Remote Address
13.1.1.3	Vlan1	1	v3.ff	0	BCAST	N/A
10.1.35.3	Vlan2	0	v3.ff	0	BCAST	N/ASwitch #

Displayed Information	Explanations
Address	Address
Interface	Interface corresponding physical interface name
Vif Index	Virtual interface index
Ver	Interface supporting version
Nbr Cnt	Neighbor count
Type	Interface type
Remote Address	Remote address

1.6.5.1.4 show ip dvmrp neighbor

Command: show ip dvmrp neighbor [{<*ifname*> <A.B.C.D> [detail]}|{ <*ifname*>[detail]}|detail]

Function: Display DVMRP neighbor.

Parameter: <*ifname*> is interface name, namely displaying neighbor information of specified interface.

Default: Do not display (Off).

Command Mode: Any Configuration Mode

Example: Display interface vlan1 neighbor on Ethernet.

Switch #show ip dvmrp neighborr

Neighbor	Interface	Uptime/Expires	Maj	Min	Cap

Address Ver Ver Flg

10.1.35.5 Vlan2 00:00:16/00:00:29 3 255 2e

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Detect the neighbor’s interface
Uptime/Expires	The neighbor uptime/expire time
Maj Ver	Major version
Min Ver	Mini version
Cap Flg	Capacity flag

1.6.5.1.5 show ip dvmrp prune

Command: show ip dvmrp prune [{group <A.B.C.D> [detail]}|{source <A.B.C.D/M> group <A.B.C.D> [detail]}|{source <A.B.C.D/M> [detail] }|detail]

Function: Display DVMRP message forwarding item.

Parameter: None

Default: Do not display

Command Mode: Any Configuration Mode

Usage Guide: This command applies to display DVMRP multicast forwarding item, namely multicast forwarding table calculated by dvmrp protocol.

Example:

Switch#show ip dvmrp prune

Flags: P=Pruned,H=Host,D=Holddown,N=NegMFC,I=Init

Source Mask Group State FCR Exptime Prune/Graft

Address Len Address Cnt ReXmit-Time

13.1.1.0 24 239.0.0.1 ..... 1 01:59:56 Off

Displayed Information	Explanations
Source Address	Source address
Mask Len	Mask length
Group Address	Group address
State	Table item state
FCR Exptime	FCR expire time
Prune/Graft ReXmit-Time	Prune expire time/ Graft retransmit time

1.6.5.1.6 show ip dvmrp route

Command: show ip dvmrp route [{<A.B.C.D/M>[detail]}|{nexthop <A.B.C.D>[detail]}|{best-match <A.B.C.D> [detail]}|detail]

Function: Prune expire time/ Graft retransmit time

Parameter: None

Default: Do not display

Command Mode: Any Configuration Mode

Usage Guide: The command applies to display DVMRP routing table item; DVMRP maintains individual unicast routing table to check RPF.

Example: Display DVMRP routiing.

Switch #show ip dvmrp route

Flags: N = New, D = DirectlyConnected, H = Holddown

Network	Flags	Nexthop Xface	Nexthop Neighbor	Metric	Uptime	Exptime
10.1.35.0/24	.D.	Vlan2	Directly Connected	1	00:11:16	00:00:00
13.1.1.0/24	.D.	Vlan1	Directly Connected	1	00:10:22	00:00:00

Displayed Information	Explanations
Network	Target net segment or address and mask
Flags	Routing state flag
Nexthop Xface	Next hop interface address
Nexthop Neighbor	Next hop neighbor
Metric	Routing metric value
Uptime	Routing uptime
Exptime	Routing expire time

1.7 DCSCM

1.7.1 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 IGMP model, 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 higer priority on TRUNK port, consequently guarantee the transmission is processed in user-specified priority in the entire network.

1.7.2 DCSCM Configuration Task List

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

1. Source Control Configuration

   Source Controll 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 earlist. 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

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 command are as follows

Command	Explanation
Global Configuration Mode	
[no] multicast destination-control **（Requied）**	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.

Next is to 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> {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 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 specified 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>

1.7.3 Command For DCSCM

1.7.3.1 access-list (Multicast Destination Control)

Command:access-list<6000-7999>{deny|permit}ip{{<source><source-wildcard>}|{host-source<source-host-ip>}|any-source}{{<destination><destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}
noaccess-list<6000-7999>{deny|permit}ip{{<source><source-wildcard>}|{host-source<source-host-ip>}|any-source}{{<destination><destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}

Function: Configure destination control multicast access-list,the "**no access-list <6000-7999>{deny|permit}ip{{<source><source-wildcard>}|{host-source<source-host-ip>}|any-source}{{<destination><destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}**" command deletes the access-list.

Parameter: <6000-7999>: destination control access-list number.

{deny|permit}: deny or permit.

<source>: multicast source address.

<source-wildcard>: multicast source address wildcard character..

<source-host-ip>: multicast source host address.

<destination>: multicast destination address.

<destination-wildcard>: multicast destination address wildcard character.

<destination-host-ip>: multicast destination host address

Default: None

Command Mode: Global Mode

Usage Guide: ACL of Multicast destination control list item is controlled by specifical ACL number from 6000 to 7999, the command applies to configure this ACL. ACL of Multicast destination control onlt needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use wildcard characterto configure address range, and also specify a host address or all address. Remarkable, "all address" is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.

Example: Switch(config)#access-list 6000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

1.7.3.2 access-list (Multicast Source Control)

Command: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}

Noaccess-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}

Function: Configure source control multicast access-list; the "**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}**" command deletes the access-list.

Parameter: **<5000-5099>**: source control access-list number.

{deny|permit}: deny or permit.

<source>: multicast source address..

<source-wildcard>: multicast source address wildcard character.

<source-host-ip>: multicast source host address.

<destination>: multicast destination address.

<destination-wildcard>: multicast destination address wildcard character.

<destination-host-ip>: multicast destination host address.

Default: None

Command Mode: Global Mode

Usage Guide: ACL of source destination control list item is controlled by specifical ACL number from 5000 to 5099, the command applies to configure this ACL. ACL of Multicast source control onlt needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use wildcard characterto configure address range, and also specify a host address or all address. Remarkable, "all address" is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.

Example: Switch(config)#access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

1.7.3.3 ip multicast destination-control access-group

Command: ip multicast destination-control access-group <6000-7999>

no ip multicast destination-control access-group <6000-7999>

Function: Configure multicast destination-control access-list used on interface, the "**no ip multicast destination-control access-group<6000-7999>**"command deletes the configuration.

Parameter: <6000-7999>: destination-control access-list number.

Default: None

Command Mode: Interface Configuration Mode

Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the interface to multicast group, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added.

Example: Switch(Config-If-Ethernet)#ip multicast destination-control access-group 6000

1.7.3.4 ip multicast destination-control access-group (sip)

Command: ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>

no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>

Function: Configure multicast destination-control access-list used on specified net segment, the "**no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>**" command deletes this configuration.

Parameter: <IPADDRESS/M>: IP address and mask length;

<6000-7999>: Destination control access-list number.

Default: None

Command Mode: Global Mode

Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING or IGMP is enabled, for adding the members to multicast group.If configuring multicast destination-control on specified net segment of transmitted igmp-report, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added. If relevant group or source in show ip igmp groups detail has been astablished before excuting the command, it needs to excute clear ip igmp groups command to clear relevant groups in Admin mode.

Example: Switch(config)#ip multicast destination-control 10.1.1.0/24 access-group 6000

1.7.3.5 ip multicast destination-control access-group (vmac)

Command: ip multicast destination-control<1-4094><macaddr>access-group <6000-7999>

no ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>

Function: Configure multicast destination-control access-list used on specified vlan-mac, the "**no ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>**" command deletes this configuration.

Parameter: <1-4094>: VLAN-ID;

<macaddr>: Transmitting source MAC address of IGMP-REPORT, the format is "xx-xx-xx-xx-xx-xx";

<6000-7999>: Destination-control access-list number.

Default: None

Command Mode: Global Mode

Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the members to multicast group.If configuring multicast destination-control to source MAC address of transmitted igmp-report, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added.

Example:

Switch(config)#ip multicast destination-control 1 00-01-03-05-07-09 access-group 6000

1.7.3.6 ip multicast policy

Command: ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>

no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos

Function: Configure multicast policy, the "**no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos**" command deletes it.

Parameter: <IPADDRESS/M>: are multicast source address, mask length, destination address, and mask length separately.

<priority>: specified priority, range from 0 to 7

Default: None

Command Mode: Global Mode

Usage Guide: The command configuration modifies to a specified value through the switch matching priority of specified range multicast data package, and the TOS is specified to the same value simultaneously. Carefully, the packet transmitted in UNTAG mode does not modify its priority.

Example: Switch(config)#ip multicast policy 10.1.1.0/24 225.1.1.0/24 cos 7

1.7.3.7 ip multicast source-control

Command: ip multicast source-control

no ip multicast source-control

Function: Configure to globally enable multicast source control, the "**no ip multicast source-control**" command restores global multicast source control disabled.

Parameter: None

Default: Disabled

Command Mode: Global Mode

Usage Guide: The source control access-list applies to interface with only enabling global multicast source control, and configure to disabled global multicast source control without configuring source control access-list on every interface. After configuring the command,

multicast data received from every interface does not have matching multicast source control list item, and then they will be thrown away by switches, namely only multicast data matching to PERMIT can be received and forwarded.

Example: Switch(config)#ip multicast source-control

1.7.3.8 ip multicast source-control access-group

Command: ip multicast source-control access-group <5000-5099>

no ip multicast source-control access-group <5000-5099>

Function: Configure multicast source control access-list used on interface, the “no ip multicast source-control access-group <5000-5099>“ command deletes the configuration.

Parameter: <5000-5099>: Source control access-list number**.**

Default: None

Command Mode: Interface Configuration Mode

Usage Guide: The command configures with only enabling global multicast source control. After that, it will match multicast data message imported from the interface according to configured access-list, such as matching: permit, the message will be received and forwarded; otherwise the message will be thrown away.

Example:

Switch(config)#inter e

Switch(Config-If-Ethernet)#ip multicast source-control access-group 5000

Switch(Config-If-Ethernet)#

1.7.3.9 multicast destination-control

Command: multicast destination-control

no multicast destination-control

Function: Configure to globally enable IPv4 and IPv6 multicast destination control. After configuring this command, IPV4 and IPv6 multicast destination control will take effect at the same time. The no operation of this command is to recover and disable the IPV4 and IPV6 multicast destination control globally.

Parameter: None.

Default: Disabled

Command Mode: Global Mode

Usage Guide: Other destination control configurations can be taken effect with only enabling global multicast destination control, the destination control access-list applies to interface, VLAN-MAC and SIP. After configuring the command, igmp snooping and IGMP match, according to above rules, when they receive IGMP REPORT to try to add interface.

Example: Switch(config)#multicast destination-control

1.7.4 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 Ethernet1/5 is allowed to transmit multicast, and the data group must be 225.1.2.3. Also, switch connected up to port Ethernet1/10 can transmit multicast data without any limit, and we can make the following configuration.

Switch(config)#access-list 5000 permit ip any host 225.1.2.3
Switch(config)#access-list 5001 permit ip any any
Switch(config)#ip multicast source-control
Switch(config)#interface ethernet1/5
Switch(Config-If-Ethernet1/5)#ip multicast source-control access-group 5000
Switch(config)#interface ethernet1/10
Switch(Config-If-Ethernet1/10)#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)

Switch(config)#ip igmp snooping
Switch(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)#ip 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.

2. 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 (Uausally 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.

1.7.5 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.

1.7.5.1 Monitor And Debug

1.7.5.1.1 show ip multicast destination-control

Command: show ip multicast destination-control [detail]

show ip multicast destination-control interface <Interfacename> [detail]

show ip multicast destination-control host-address <ipaddress> [detail]

show ip multicast destination-control <vlan-id> <mac-address> [detail]

Function: Display multicast destination control

Parameter: detail: expresses if it display information in detail or not..

<Interfacename>: interface name or interface aggregation name, such as Ethernet1/1, port-channel 1 or ethernet1/1..

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays multicast destination control rules of configuration, including detail option, and access-list information applied in detail.

Example:

switch (config)#show ip multicast destination-control

ip multicast destination-control is enabled

ip multicast destination-control 11.0.0.0/8 access-group 6003

ip multicast destination-control 1 00-03-05-07-09-11 access-group 6001

multicast destination-control access-group 6000 used on interface Ethernet

1.7.5.1.2 show ip multicast destination-control access-list

Command: show ip multicast destination-control access-list

show ip multicast destination-control access-list <6000-7999>

Function: Display destination control multicast access-list of configuration.

Parameter: <6000-7999>: access-list number.

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays destination control multicast access-list of configuration.

Example:

Switch# sh ip multicast destination-control acc

access-list 6000 deny ip any-source any-destination

access-list 6000 deny ip any-source host-destination 224.1.1.1

access-list 6000 deny ip host-source 2.1.1.1 any-destination

access-list 6001 deny ip host-source 2.1.1.1 225.0.0.0 0.255.255.255

access-list 6002 permit ip host-source 2.1.1.1 225.0.0.0 0.255.255.255

access-list 6003 permit ip 2.1.1.0 0.0.0.255 225.0.0.0 0.255.255.255

1.7.5.1.3 show ip multicast policy

Command: show ip multicast policy

Function: Display multicast policy of configuration

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays multicast policy of configuration

Example:

Switch#show ip multicast policy

ip multicast-policy 10.1.1.0/24 225.0.0.0/8 cos 5

1.7.5.1.4 show ip multicast source-control

Command: show ip multicast source-control [detail]

show ip multicast source-control interface <Interfacename> [detail]

Function: Display multicast source control configuration

Parameter: detail: expresses if it displays information in detail.

<Interfacename>: interface name, such as Ethernet 1/1 or ethernet 1/1.

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays multicast source control rules of configuration, including detail option, and access-list information applied in detail

Example:

Switch#show ip multicast source-control detail

ip multicast source-control is enabledInterface Ethernet use multicast source control access-list 5000

access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255

1.7.5.1.5 show ip multicast source-control access-list

Command: show ip multicast source-control access-list

show ip multicast source-control access-list <5000-5099>

Function: Display source control multicast access-list of configuration

Parameter: <5000-5099>: access-list number

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays source control multicast access-list of configuration

Example:

Switch#sh ip multicast source-control access-list

access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255

1.8 IGMP

1.8.1 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 are 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 very 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.

1.8.2 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 is not specific command 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 | ip pim dense-mode | ip pim sparse-mode	Enable IGMP Protocol, the corresponding commands “**no ip dvmrp | 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.

1.8.3 Command For IGMP

1.8.3.1 ip igmp access-group

Command:ip igmp access-group {<*acl_num* | *acl_name*>}

no ip igmp access-group

Function: Configure interface to filter IGMP group; the "**no ip igmp access-group**" command cancels the filter condition

Parameter: {<acl_num | acl_name>} is SN or name of access-list, value range of **acl_num** is from 1 to 99.

Default: Default no filter condition

Command Mode: Interface Configuration Mode

Usage Guide: Configure interface to filter groups, permit or deny some group joining.

Example: Configure interface vlan1 to permit group 224.1.1.1, deny group 224.1.1.2.

Switch (config)#access-list 1 permit 224.1.1.1 0.0.0.0

Switch (config)#access-list 1 deny 224.1.1.2 0.0.0.0

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp access-group 1

1.8.3.2 ip igmp immediate-leave

Command: ip igmp immediate-leave group-list {<number>|<name>}

no ip igmp immediate-leave

Function: Conifgure IGMP working in immediate-leave mode, that is, when the host transmits member identity report of equivalent to leave a group, router does not transmit query, it directly

confirms there is no member of this group in subnet; the "**no ip igmp immediate-leave**" command cancels immediate-leave mode.

Parameter: ***<number>*** is access-list SN, value is from 1 to 99.

<name> is access-list name.

Default: Interface default and no immediate-leave group of configuration after finished product

Command Mode: Interface Configuration Mode

Usage Guide: The command only can apply in only one host condition in subnet.

Example: Configure immediate-leave mode on access-group list 1

Switch (Config-if-Vlan1)#ip igmp immediate-leave group-list 1

Switch (Config-if-Vlan1)#

1.8.3.3 ip igmp join-group

Command:ip igmp join-group <*A.B.C.D* >

no ip igmp join-group <*A.B.C.D* >

Function: Configure interface to join some IGMP group; the "no ip igmp join-group" command cancels this join

Parameter: ***<A.B.C.D>:*** is group address

Default: Do not join

Command Mode: Interface Configuration Mode

Usage Guide: When the switch is the HOST, the command configures HOST to join some group; that is, if configuring the interface join-group 224.1.1.1, it will transmit IGMP member report including group 224.1.1.1 when the switch receives IGMP group query transmitted by other switches. Carefully, it is the difference between the command and **ip igmp static-group** command.

Example: Configure join-group 224.1.1.1 on interface vlan1.

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp join-group 224.1.1.1

1.8.3.4 ip igmp last-member-query-interval

Command: ip igmp last-member-query-interval <interval>

no ip igmp last-member-query-interval

Function: Configure interval of specified group query transmtting on interface; the "**no ip igmp last-member-query-interval**" command cancels the value of user manual configuration, and restores default value.

Parameter: ***<interval>*** is interval of specified group query, range from 1000ms to 25500ms; the value is integer times of 1000ms, namely if input value is not integer times of 1000ms, the system autometically changes to integer times of 1000ms.

Default: 1000ms

Command Mode: Interface Configuration Mode

Example: Configure interface vlan1 IGMP last-member-query-interval to 2000.

Switch (config)#int vlan 1

Switch (Config-if-vlan1)#ip igmp last-member-query-interval 2000

1.8.3.5 ip igmp limit

Command: ip igmp limit <state-count>

no ip igmp limit

Function: Configure limit IGMP state-count on interface; the "**no ip igmp limit**" command cancels the value of user manual configuration, and restores default value.

Parameter: ***<state-count>*** is maximum IGMP state reserved by interface, range from 1 to 65000

Default: Default: 0, no limit.

Command Mode: Interface Configuration Mode

Usage Guide: After configuring mamimum state state-count, interface only saves states which are not more than state-count groups and sources. If it reaches upper limit of state-count, it does not deal with when receiving related new group member identity report. If it has saved some IGMP group states before configuring the command, it deletes all of the states, and then immediately transmits IGMP general query to collect the member identity report which is not more than state-count group. Static state and static source are not in the limit

Example: Configure interface vlan1 IGMP limit to 4000.

Switch (config)#int vlan 1

Switch (Config-if-vlan1)#ip igmp limit 4000

1.8.3.6 ip igmp query-interval

Command:ip igmp query-interval <*time_val*>

no ip igmp query-interval

Function: Configure interval of periodically transmitted IGMP query information; the "**no ip igmp query-interval**" command restores default value.

Parameter: ***<time_val>*** is interval of periodically transmitted IGMP query information, value range from 1s to 65535s.

Default: Default interval of periodically transmitted IGMP query information to 125s.

Command Mode: Interface Configuration Mode

Usage Guide: Periodically transmitting IGMP query information on interface when some interface enables some group multicast protocol. The command applies to configure this query period time.

Example: Configure interval of periodically transmitted IGMP query message to 10s

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp query-interval 10

1.8.3.7 ip igmp query-max-response-time

Command:ip igmp query-max-response-time <*time_val*>

no ip igmp query- max-response-time

Function: Configure IGMP query-max-response-time of interface; the "**no ip igmp query-max-response-time**" command restores default value.

Parameter: <***time_val***> is IGMP query-max-response-time of interface, value range from 1s to 25s

Default: Default: 10s.

Command Mode: Interface Configuration Mode

Usage Guide: After the switch receives a query message, the host will configure a timer for its affiliated every multicast group, the value of timer is selected random from 0 to maximum response time, the host will transmit member report message of the multicast group. Reasonable configuring maximum response time, it can make host quickly response query message. The router can also quickly grasp the status of multicast group member.

Example:onfigure the maximum period responding to the IGMP query messages to 20s

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp query- max-response-time 20

1.8.3.8 ip igmp query-timeout

Command:ip igmp query-timeout <*time_val*>

no ip igmp query-timeout

Function: Configure IGMP query timeout of interface; the "**no ip igmp query-timeout**" command restores default value.

Parameter: <***time_val***> is IGMP query-timeout, value range from 60s to 300s.

Default: Default: 255s.

Command Mode: Interface Configuration Mode

Usage Guide: When multi-running IGMP switches are exist on sharing network, a switch will be voted as query processor on the sharing network, and other switches will be a timer monitoring the state of query processor; It still does not receive query message transmitting by query processor over query time-out, thus it re-votes another switch as new query processor.

Example: Configure timeout of IGMP query message on interface to 100s.

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp query-timeout 100

1.8.3.9 ip igmp static-group

Command:ip igmp static-group <*A.B.C.D* > [source <*A.B.C.D* >]

no ip igmp static -group <*A.B.C.D* > [source <*A.B.C.D* >]

Function: Configure interface to join some IGMP static group; the “no ip igmp static-group” command cancels this join.

Parameter: *<A.B.C.D>* is group address;

Source ***<A.B.C.D>*** expresses SSM source address of configuration.

Default: Do not join static group

Command Mode: Interface Configuration Mode

Usage Guide: When configuring some interface to join some static group, it will receives about the multicast package of the static group whether the interface has a real receiver or not; that is, if configuring the interface to join static group 224.1.1.1, the interface always receives about multicast packet about group 224.1.1.1 whether the interface has a receiver or not. Carefully, it is the difference between the command and ip igmp join-group command.

Example: Configure static-group 224.1.1.1 on interface vlan1.

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp static-group 224.1.1.1

1.8.3.10 ip igmp version

Command: ip igmp version <*version*>

no ip igmp version

Function: Configure IGMP version on interface; the “**no ip igmp version**” command restores default value.

Parameter: <***version***> is IGMP version of configuration, currently supporting version 1, 2 and 3.

Default: Default: version 2.

Command Mode: Interface Configuration Mode

Usage Guide: The command mainly applies to supply upward compatibility of the different version; it is not communicated between version 1 and version 2, therefore it must configure to the same version IGMP in the same network. When other routers which are not upgraded to IGMPv3 on interface-connected subnet need to join member identity collection of subnet IGMP together, the interface is configured to corresponding version.

Example: Configure IGMP on interface to version 3.

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp version 3

1.8.4 IGMP Configuration Example

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.

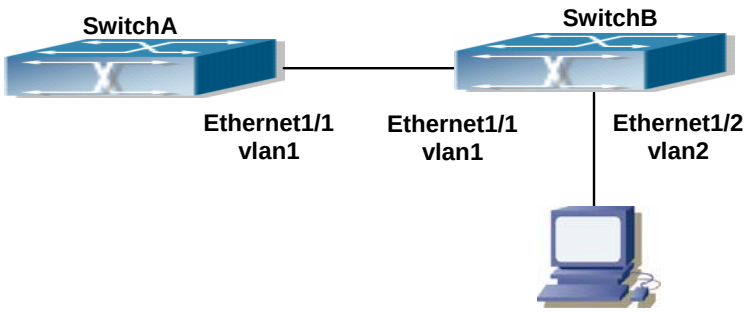


Fig 1-8 IGMP Network Topology Diagram

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

1.8.5 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.

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

1.8.5.1 Monitor and debug command

1.8.5.1.1 debug igmp event

Command: debug igmp event

no debug igmp event

Function: Enable debugging switch of IGMP event; the "**no debug igmp event**" command disenables the debugging switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable debugging switch if querying IGMP event information

Example:

Switch# debug igmp event

igmp event debug is on

Switch# 01:04:30:56: IGMP: Group 224.1.1.1 on interface vlan1 timed out

1.8.5.1.2 debug igmp packet

Command: debug igmp packet

no debug igmp packet

Function: Enable debugging switch of IGMP message information; the "**no debug igmp packet**" command disenables the debugging switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable the debugging switch if querying IGMP message information.

Example:

Switch# debug igmp packet

igmp packet debug is on

Switch #02:17:38:58: IGMP: Send membership query on dvmrp2 for 0.0.0.0

02:17:38:58: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0

.0.0

02:17:39:26: IGMP: Send membership query on vlan1 for 0.0.0.0

02:17:39:26: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0

.0.0

1.8.5.1.3 show ip igmp groups

Command: show ip igmp groups [<*A.B.C.D*>] [*detail*]

Function: Display IGMP group information

Parameter: <*group_addr*> is group address, namely querying specified group information; Detail expresses group information in detail

Default: Do not display

Command Mode: Admin Mode

Example:

Switch (config)#show ip igmp groups

IGMP Connected Group Membership (2 group(s) joined)

Group Address	Interface	Uptime	Expires	Last Reporter
226.0.0.1	Vlan1	00:00:01	00:04:19	1.1.1.1
239.255.255.250	Vlan1	00:00:10	00:04:10	10.1.1.1

Switch#

Displayed Information	Explanations
Group Address	Multicast group IP address
Interface	Interface affiliated with multicast group
Uptime	Multicast group uptime
Expires	Multicast group expire time
Last Reporter	Last reporter to the host of the multicast group

Switch (config)#show ip igmp groups 234.1.1.1 detail

IGMP Connect Group Membership (2 group(s) joined)

Flags: SG - Static Group, SS - Static Source, SSM - SSM Group, V1 - V1 Host Pres

ent, V2 - V2 Host Present

Interface: Vlan1

Group: 234.1.1.1

Flags:

Uptime: 00:00:19

Group Mode: INCLUDE

Last Reporter: 10.1.1.1

Exptime: stopped

Source list: (2 members S - Static)

Source Address	Uptime	v3 Exp	Fwd	Flags
1.1.1.1	00:00:19	00:04:01	Yes	
2.2.2.2	00:00:19	00:04:01	Yes	

Displayed Information	Explanations
Group	Mutlicast group IP address
Interface	Interface affiliated with Mutlicast group
Flags	Group property flag
Uptime	Mutlicast group uptime
Group Mode	Group mode, including INCLUDE and EXCLUDE. Group V3 will be available, group V1 and group V2 are regards as EXCLUDE mode.
Exptime	Mutlicast group expire time
Last Reporter	Last reporter to the host of the Mutlicast group
Source Address	Source address of this group
V3 Exp	Source expire time
Fwd	If the data of the source is forwarded or not.
Flags	Source property flag

1.8.5.1.4 show ip igmp interface

Command: show ip igmp interface [<*ifname*>]

Function: Display related IGMP information on interface.

Parameter: <*ifname*> is interface name, namely displaying IGMP information of specified interface.

Default: Do not display

Command Mode: Admin Mode

Example: Display interface vlan1 IGMP message on Ethernet.

Switch (config)#show ip igmp interface Vlan1

Interface Vlan1(2005)

Index 2005

Internet address is 10.1.1.2

IGMP querier

IGMP current version is V3, 2 group(s) joined

IGMP query interval is 125 seconds

IGMP querier timeout is 255 seconds

IGMP max query response time is 10 seconds

Last member query response interval is 1000 ms

Group Membership interval is 260 seconds

IGMP is enabled on interface

1.9 IGMP Proxy

1.9.1 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.

1.9.2 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 assistant parameter.

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	Exlanation
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 datagrams. The no from of this command will disable the configuration.

1.9.3 Commands for IGMP Proxy

1.9.3.1 debug igmp proxy all

Command：debug igmp proxy all

no debug igmp proxy all

Function: Enable all the debugging switches of IGMP Proxy; the "**no debug igmp proxy all**" command disenables all the debugging switches.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guide: Use to enable debugging switches of IGMP Proxy, it can display IGMP packet, event, timer, which disposed in the switch.

Example：

Switch#debug igmp proxy all

1.9.3.2 debug igmp proxy event

Command：debug igmp proxy event

no debug igmp proxy event

Function: Enable/Disable debug switch of igmp proxy event.

Parameter：None.

Default: Disabled.

Command Mode：Admin Mode and Global Mode.

Usage Guide: Enable debugging switch if querying event information of igmp proxy.

Example：

Switch#debug igmp proxy event

1.9.3.3 debug igmp proxy mfc

Command：debug igmp proxy mfc

no debug igmp proxy mfc

Function: Enable/Disable debug switch of igmp proxy multicast forwarding cache.

Parameter：None.

Default: Disabled.

Command Mode：Admin Mode and Global Mode.

Usage Guide: Enable igmp proxy mfc debug switch and display multicast information created and distributed.

Example：

Switch#debug igmp proxy mfc

1.9.3.4 debug igmp proxy packet

Command：debug igmp proxy packet

no debug igmp proxy packet

Function: Enable/Disable debug switch of IGMP Proxy.

Parameter：None.

Default: Disabled.

Command Mode：Admin Mode and Global Mode.

Usage Guide: Enable the debugging switch, you can monitor the packets. receiving/sending of igmp proxy.

Example：

Switch#debug igmp proxy packet

1.9.3.5 debug igmp proxy timer

Command：**debug igmp proxy** t**imer**

no debug igmp proxy timer

Function: Enable/Disable each timer of igmp proxy.

Parameter：None.

Default: Disabled.

Command Mode：Admin Mode and Global Mode.

Usage Guide: The command is used for enable the IGMP proxy timer debugging switch which appointed.

Example：

Switch#debug ip igmp proxy timer

1.9.3.6 ip igmp proxy

Command：**ip igmp proxy**

no ip igmpp proxy

Function: Enable the IGMP Proxy function; The "**no ip igmpp proxy**" command disables this function.

Command Mode：Global Mode.

Default：The switch disable IGMP Proxy by default.

Usage Guide: Use this command to enable IGMP Proxy, and configure one upstream port and at least one downstream port under interface configuration mode if make the IGMP Proxy operate.

Example：Enable IGMP Proxy under Global Mode.

Switch(config)#ip igmp proxy

1.9.3.7 ip igmp proxy aggregate

Command：**ip igmp proxy aggregate**

no ip igmp proxy aggregate

Function: To configure non-query downstream ports to be able to aggregate the IGMP operations.

Command Mode：Global Mode.

Default: The non-query downstream ports are not to be able to aggregate the IGMP operations in default.

Usage Guide: By default non-query downstream ports cannot aggregate and redistribute the multicast messages. This command is used to enable all the downstream ports to be able to aggregate and redistribute the multicast dataflow.

Example：

Switch(config)#ip igmp proxy aggregate

1.9.3.8 ip igmp proxy downstream

Command：**ip igmp proxy downstream**

no ip igmp proxy downstream

Function: Enable the appointed IGMP Proxy downstream port function. The "**no ip igmp proxy upstream**" disables this function.

Command Mode：Interface Configuration Mode.

Default：Disabled.

Usage Guide: To configure the interface to function as the downstream port of IGMP proxy. In order to make IGMP proxy work, at least one upstream interface should be configured. The no form of this command will disable the configuration.

Example: Enable IGMP Proxy downstream port function in interface vlan1 under interface configuration mode.

Switch(config)#interface vlan 2

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

1.9.3.9 ip igmp proxy limit

Command：**ip igmp proxy limit {group <*g_limit*> | source <*s_limit*>}**

no ip igmp proxy limit

Function: 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.

Parameter：***g_limit***：<1-500>, the group number limitation.

s_limit：<1-500>, the source number limitation.

Command Mode：Global Mode.

Default: Most 50 groups in default, and most 40 sources in one group.

Usage Guide: If the group number limitation is exceeded, new group membership request will be rejected. This command is used to prevent malicious group membership requests.

Example：

Switch(config)#ip igmp proxy limit group 30 source 20

1.9.3.10 ip igmp proxy multicast-source

Command：ip igmp proxy multicast-source

no ip igmp proxy multicast-source

Function: To configure the port as downstream port for the source of multicast datagram. the no from of this command disables the configuration.

Command Mode： Interface Configuration Mode.

Default: The downstream port is not for the source of multicast datagram.

Usage Guide: When a downstream port is configured as the multicast source port, the switch will be able to receive multicast data flow from that port, and forward it to the upstream port. To make this command function, the multicast router which is connected to the upstream port of the switch, should be configured to view the multicast source from the upstream port is directly connected to the router.

Example： Enable igmp proxy multicast-source in downstream port vlan1.

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip igmp proxy multicast-source

1.9.3.11 ip igmp proxy unsolicited-report interval

Command：ip igmp proxy unsolicited-report interval <value>

no ip igmp proxy unsolicited-report interval

Function: To configure how often the upstream ports send out unsolicited report.

Parameter: The interval is between <1, 5> seconds for the upstream ports send out unsolicited report.

Command Mode： Global Mode.

Default: The interval is 1 second for the upstream ports send out unsolicited report in default.

Usage Guide: The upstream ports re-transmit the unsolicited reports in order that the router will not miss the report packet due to link down or packet loss. This command configures the interval for re-transmition.

Example：

Switch(config)#ip igmp proxy unsolicited-report interval 3

1.9.3.12 ip igmp proxy unsolicited-report robustness

Command：ip igmp proxy unsolicited-report robustness <value>

no ip igmp proxy unsolicited-report robustness

Function: To configure the retry times of upstream ports' sending unsolicited reports. The no

form of this command will restore the default value.

Parameter：*value* ：<2~10>. The retry times for upstream ports' sending unsolicited reports is limited between 2 and 10.

Command Mode：Global Mode.

Default: Retry times is 2 by default.

Usage Guide: The upstream ports re-transmit the unsolicited reports in order that the router will not miss the report packet due to link down or packet loss.

Example：

Switch(config)#ip igmp proxy unsolicited-report robustness 3

1.9.3.13 ip igmp proxy upstream

Command：ip igmp proxy upstream

no ip igmp proxy upstream

Function: Enable the appointed IGMP Proxy upstream port function. The "**no ip igmp proxy upstream**" disables this function.

Command Mode：Interface Configuration Mode.

Default: Disabled.

Usage Guide: To configure the interface to function as the upstream port of IGMP proxy. In order to make IGMP proxy work, at least one downstream interface should be configured. The no form of this command will disable the configuration.

Example: Enable IGMP Proxy upstream port function in interface vlan1 under interface configuration mode.

Switch(config)#interface vlan 1

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

1.9.3.14 ip multicast ssm

Command：ip multicast ssm range {<1-99>| default}

no ip multicast ssm

Function: To configure the address range for IGMP proxy ssm multicast groups; the no form of this command will delete the ssm multicast groups.

Parameter：default show the address range 232/8 for ssm multicast groups.

<access-list-number> is the applied access list number, range is 1-99.

Command Mode：Global Mode.

Default: The default address range is 232/8 for ssm multicast groups.

Usage Guide: The command configures the address filter for multicast group membership request. The request for the specified address ranges will be dropped. This command is also available for both the IGMP proxy and PIM configuration. To be mentioned, this command cannot be applied with DVMRP configuration.

Example：To enable SSM configuration on the switch, and specify the address in access-list 23 as the filter address for SSM.

Switch(config)#access-list 23 permit host-source 224.1.1.1

Switch(config)#ip multicast ssm range 23

1.9.3.15 ip pim bsr-border

Command：**ip pim bsr-border**

no ip pim bsr-border

Function: To configure the PIM enabled port to consider all the multicast source is directly connected. The no form of this command will remove the configuration.

Command Mode：Interface Configuration Mode

Default: Disabled.

Usage Guide: Configuring the multicast source to be considered as directly connected for the PIM enabled port is used to determine the identity of DR and ORIGINATOR.

Example：To configure PIM enabled vlan 2 as the port for BSR BORDER. For all the multicast flow from external network through vlan 2, the switch will consider the multicast source is directly connected to the switch.

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)#ip pim bsr-border

1.9.3.16 show debugging igmp proxy

Command：**show debugging igmp proxy**

Command Mode：Admin Mode.

Usage Guide：The status of debug switch of igmp proxy.

Example：

Switch(config)#show debugging igmp proxy

IGMP PROXY debugging status:

IGMP PROXY event debugging is on

IGMP PROXY packet debugging is on

IGMP PROXY timer debugging is on

IGMP PROXY mfc debugging is on

1.9.3.17 show ip igmp proxy

Command：**show ip igmp Proxy**

Command Mode：Admin Mode

Usage Guide: To show configuration for igmp proxy about whether the igmp proxy is enabled globally, and whether upstream ports and downstream ports has been configured.

Example：

Switch(config)#show ip igmp Proxy

IGMP PROXY MRT running: Enabled
 Total active interface number: 2

Global igmp proxy configured: YES
Total configured interface number: 2
Upstream Interface configured: YES
  Upstream Interface Vlan1(2005)
Upstream Interface configured: YES
  Downstream Interface Vlan2(2006)

Show Information	Explanation
IGMP PROXY MRT running	Whether the protocol is running.
Total active interface number	Number of active upstream and downstream ports.
Global igmp proxy configured	Whether global igmp proxy is enabled.
Upstream Interface configured	Whether upstream port is configured.
Upstream Interface Vlan	The vlan which the upstream port belongs to.
Upstream Interface configured	Whether downstream port is configured.
Downstream Interface Vlan	The vlan which the downstream port belongs to.

1.9.3.18 show ip igmp proxy mroute

Command：show ip igmp Proxy mroute

Command Mode： Admin Mode

Usage Guide: Display the status information of igmp proxy mroute, and information about the mrt node.

Example：

Switch(config)#show ip igmp proxy mroute

IP Multicast Routing Table

(*,G) Entries: 0
(S,G) Entries: 2

(1.1.1.2, 225.0.0.1)
 Local_include_olist ..l.....

Local_exclude_olist .....
Outgoing ..o.....

(1.1.1.3, 225.0.0.1)
Local_include_olist ..l.....
Local_exclude_olist .....
Outgoing ..o.....

Show Information	Explanation
Entries	The counts of each item
Local_include_olist	index for local include olist.
Local_exclude_olist	index for local exclude olist.
Outgoing	Final outgoing index of multicast data(S, G)

1.9.3.19 show ip igmp proxy upstream groups

Command：show ip igmp proxy upstream groups {A.B.C.D}

Command Mode： Admin Mode

Usage Guide: To show the group membership information of the upstream port. If the group is not specified, information of all groups will be displayed. Otherwise, only the specified will be displayed.

Example：

Switch(config)#show ip igmp proxy upstream groups

IGMP PROXY Connect Group Membership
Groups Filter-mode source
224.1.1.1 INCLUDE 192.168.1.136
226.1.1.1 *

Show Information	Explanation
Groups	IP addresses of multicast groups
Filter-mode	Filter-mode of the multicast group
source	Source hold by the multicast group

1.9.4 Examples of IGMP Proxy

Example 1： IGMP Proxy function.

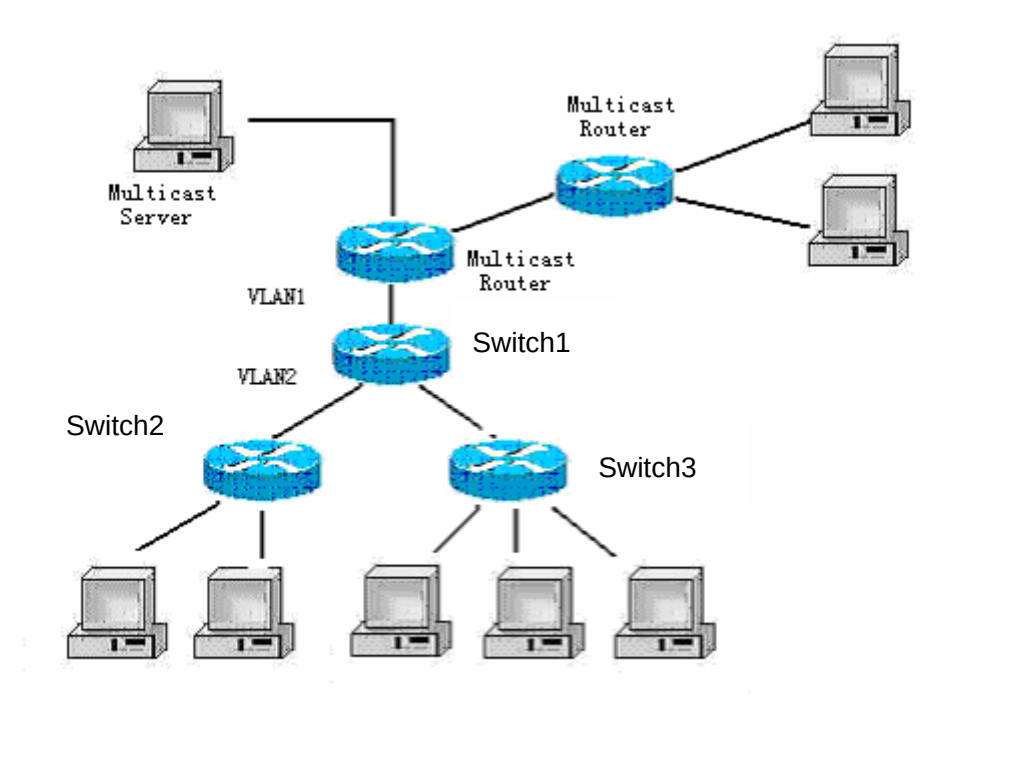


Fig 1-9 IGMP Proxy Topology Diagram

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 dataflows from upstream ports and redistribute 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

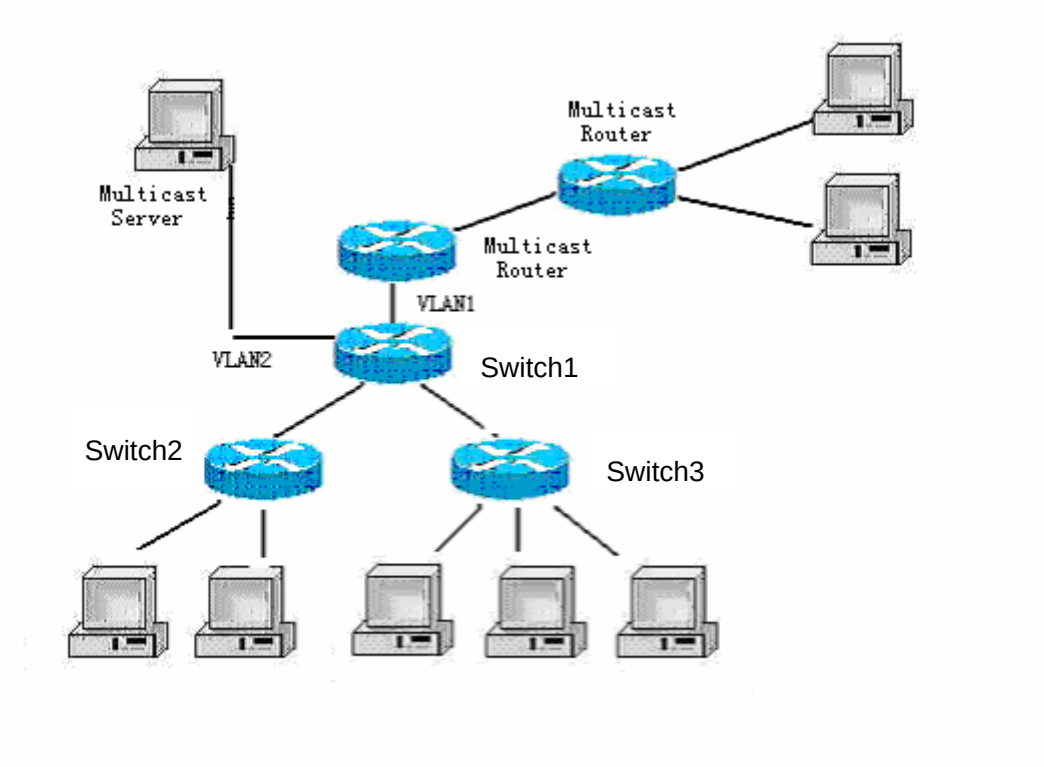


Fig 1-10 IGMP proxy for multicast sources from downstream ports

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 Switch 1. 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.

1.9.5 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 noted 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 remain unsolved, please use debug igmp proxy and other debugging command and copy the DEBUG message within 3 minutes, send the recorded message to the technical server center.

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、 Start PIM-DM (Required)

2、 To configure static multicast routing entries(optional)

3、 Configure PIM-DM auxiliary parameters (Optional)

Configure PIM-DM interface parameters

Configure PIM-DM hello message interval time

To configure the boundary interfaces.

To configure the management boundary

4、 Shut down PIM-DM protocol

1. Start PIM-DM Protocol

It's easy to make basic configuration of the PIM-DM routing protocol in EdgeCore layer 3 switch, only need to turn on PIM multicast switch in Global Mode and turn on PIM-DM switch on

relevant interface.

Command	**Explanation**
Global Mode	
ipv6 pim multicast-routing	Enable PIM-DM Protocol (but below commands are required to really function PIM-DM protocol)

And then turn on PIM-DM switch on the interface

Command	**Explanation**
Port Configuration Mode	
ipv6 pim dense-mode	Start PIM-DM Protocol of the interface (Required)

2．To configure static multicast routing entries

Command	Notes
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 PIM-DM Auxiliary Parameters

（1）Configure PIM-DM Interface Parameters

1) Configure PIM-DM hello message interval time

Command	**Explanation**
Port Configuration Mode	
ipv6 pim hello-interval < *interval*> **no ipv6 pim hello-interval**	Configure PIM-DM hello message interval time; the NO operation of this command restores the default value.

2) Configure PIM-DM state-refresh message interval time

Command	**Explanation**
Port Configuration Mode	
ipv6 pim state-refresh origination-interval **no ipv6 pim state-refresh origination-interval**	Configure PIM-DM state-refresh message interval time; the NO operation of this command restores the default value.

3）To configure the boundary interfaces

Command	Notes
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）To configure the management boundary

Command	Notes
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. The no form of this command will remove the configuration.

4. Shut down PIM-DM Protocol

Command	**Explanation**
Port Configuration Mode	
no ipv6 pim dense-mode	Turn off PIM-DM protocol of the interface
Global Mode	
no ipv6 pim multicast-routing	Shut down PIM-DM Protocol in global mode.

2.1.3 Command for PIM-DM6

2.1.3.1 ipv6 mroute

Command: 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>*]

Function: To configure static multicast entry. The no command is to delete some static multicast entries or some egress interfaces.

Parameter: <X:X::X:X> <X:X::X:X> are the source address and group address of multicast. <ifname>, the first one is ingress interface, follow is egress interface.

Command Mode: Global Mode

Default: None.

Usage Guide: The <ifname> should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be fordwarded.

Example:

Switch(config)#ipv6 mroute 2001::1 ff1e::1 v10 v20 v30

Switch(config)#

2.1.3.2 ipv6 pim bsr-border

Command: ipv6 pim bsr-border

no ipv6 pim bsr-border

Function: To configure or delete PIM6 BSR-BORDER interface.

Parameter: None

Default: Non-BSR-BORDER

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the interface as the BSR-BORDER. If configured, BSR related messages will not received from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.

Example:

Switch(Config-if-Vlan1)#ipv6 pim bsr-border

Switch(Config-if-Vlan1)#

2.1.3.3 ipv6 pim dense-mode

Command: ipv6 pim dense-mode

no ipv6 pim dense-mode

Function: Enable PIM-DM protocol on interface; the "**no ipv6 pim dense-mode**" command disenables PIM-DM protocol on interface.

Parameter: None

Default: Disable PIM-DM protocol

Command Mode: Interface Configure Mode

Usage Guide: The command will be taken effect, executing ipv6 multicast-routing in Global Mode. Don't support multicast protocol mutual operation, namely can't synchronously enable dense mode and sparse mode in one swtich. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Enable PIM-DM protocol on interface vlan1.

Switch (config)#ipv6 pim multicast-routing

Switch (config)#interface vlan 1

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

2.1.3.4 ipv6 pim dr-priority

Command: ipv6 pim dr-priority <*priority*>

no ipv6 pim dr-priority

Function: Configure, cancel and change priority value of interface DR. The same net segment border nodes vote specified router DR in this net segment through hello messages, the “no ipv6 pim dr-priority” restores default value.

Parameter: < *priority*> priority, value range from 0 to 4294967294

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Value range is from 0 to 4294967294, the bigger value, the more priority. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Switch (config)# interface vlan 1

Switch(Config-if-Vlan1)ipv6 pim dr-priority 100

2.1.3.5 ipv6 pim exclude-genid

Command: **ipv6 pim exclude-genid**

no ipv6 pim exclude-genid

Function: The command make Hello message transmitted by PIM-SM exclude Genid option, the “**no ipv6 pim exclude-genid**” restores default value.

Parameter: None

Default: Hello message includes Genid option

Command Mode: Interface Configuration Mode

Usage Guide: The command is used to interactive with old Cisco IOS Version. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure hello messages transmitted by switch to exclude Genid option.

Switch(Config-if-Vlan1)#ipv6 pim exclude-genid

2.1.3.6 ipv6 pim hello-holdtime

Command: ipv6 pim hello-holdtime <*value*>

no ipv6 pim hello-holdtime

Function: Configure and cancel Holdtime item value in Hello message, the value describes neighbor overtime. If it goes over the time and does not receive hello message of the neighbor, the register of the neighbor will be delete.

Parameter: <*value*> is configure time of holdtime.

Default: Difine 3.5 times of Hello_interval, and default hello_interval as 30s, so default value of hello_holdtime is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If no setting, hellotime will default current 3.5 times of Hello_interval. If setting hellotime is less than current hello_interval, this setting will be declined. When updating hello_interval every time, hello_holdtime will be also update based on these rules below: if hello_holdtime does not be configured, or if hello_holdtime configured is less than current hello_interval, hello_holdtime will be modified to 3.5 times Hello_interval, otherwise, keeps configured value. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure hello holdtime setting on interface vlan1 to 10.

Switch (config)# interface vlan1

Switch (Config -if-Vlan1)#ipv6 pim hello-holdtime 10

2.1.3.7 ipv6 pim hello-interval

Command: ipv6 pim hello-interval < *interval*>

no ipv6 pim hello-interval

Function: Configure interface PIM-DM hello message interval; the "**no ipv6 pim hello-interval**" command restores default value.

Parameter: < *interval*> is interval of periodically transmitted PIM-DM hello message, value range from 1s to 18724s.

Default: Default interval of periodically transmitted PIM-DM hello message as 30s.

Command Mode: Interface Configuration Mode

Usage Guide: Hello message makes PIM-DM switch mutual location, and ensures neighborship. PIM-DM switch announces existence itself by periodically transmitting hello messages to neighbors. If it doesn't receive hello messages from neighbors in regulation time, it confirms that the neighbors were lost. Configuration time is not more than neighbor overtime. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure PIM-DM hello interval on interface vlan1

Switch (config)#interface vlan1

Switch(Config-if-Vlan1)#ipv6 pim hello-interval 20

2.1.3.8 ipv6 pim multicast-routing

Command: ipv6 pim multicast-routing

no ipv6 pim multicast-routing

Function: Globally enable PIM-DM protocol; the "**no ipv6 pim multicast-routing**" command disenables PIM-DM protocol.

Parameter: None

Default: Disable PIM-DM protocol

Command Mode: Global Mode

Usage Guide: Ipv6 pim can enable only after executing this command.

Example: Globally enable PIM-DM protocol

Switch (config)#ipv6 pim multicast-routing

2.1.3.9 ipv6 pim neighbor-filter

Command: ipv6 pim neighbor-filter <a*cess-list-name*>

no ipv6 pim neighbor-filter <a*cess-list-name*>

Function: Configure neighbor access-list. If filtered by list and connected the neighbor, the connection immediately was breaken. If no connection, the connection can be established.

Parameter: *<access-list-name>* is an applied access-list name

Default: No neighbor filter configuration

Command Mode: Interface Configuration Mode

Usage Guide: If it is not necessary for partner to establish neighborship, the command can filter pim message of partner. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure access-list of pim neighbor on interface vlan1

Switch (Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter

Switch (config)# ipv6 access-list myfilter deny fe80:20e:cff:fe01:facc

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

2.1.3.10 ipv6 pim scope-border

Command: ipv6 pim scope-border [<*500-599*>|<*acl_name*>]

no ipv6 pim scope-border

Function: To configure or delete management border of PIM6.

Parameters: <1-99> is the ACL number for the management border.

<acl_name> is the ACL name for the management border.

Default: Not management border. If no ACL is specified, the default management border will be used.

Command Mode: Interface Configuration Mode

Usage Guide: To configure the management border and the ACL for the PIM protocol. The multicast data flow will not be forwarded to the SCOPE-BORDER.

Example:

Switch(Config-if-Vlan2)#ipv6 pim scope-border 503

Switch(Config-if-Vlan2)#

2.1.3.11 ipv6 pim state-refresh origination-interval

Command: ipv6 pim state-refresh origination-interval <interval>

no ipv6 pim state-refresh origination-interval

Function: Configure transmission interval of state-refresh message on interface. The “no ipv6 pim state-refresh origination-interval” command restores default value.

Parameter: <*interval*> message transmission interval value is from 4s to 100s.

Default: 60s

Usage Guide: The first-hop router periodically transmits stat-refresh messages to maintain PIM-DM list ltems of all the downstream routers. The command can modify origination interval of state-refresh messages. Usually do not modify relevant timer interval. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure transmission interval of state-refresh message on interface vlan1 to 90s.

Switch (Config-if-Vlan1)#ipv6 pim state-refresh origination-interval 90

Switch (Config-if-Vlan1)#

2.1.4 PIM-DM 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.

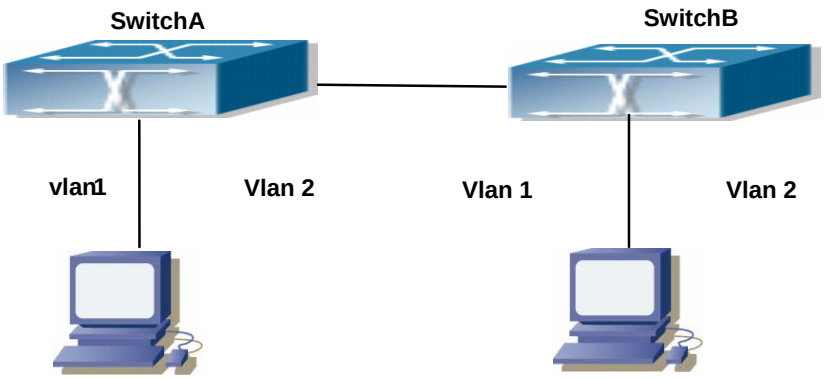


Fig 2-1PIM-DM Typical Environment

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

2.1.5 PIM-DM Troubleshooting Help

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.

2.1.5.1 Monitor and debug command

2.1.5.1.1 debug ipv6 pim timer sat

Command: debug ipv6 pim timer sat
no debug ipv6 pim timer sat

Function: Enable debug switch of PIM-DM source activity timer information in detail; the "**no debug ipv6 pim timer sat**" command disenables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable the switch, and display source activity timer information in detail.

Example: Switch # debug ipv6 pim timer sat

Remark: Other debug switches in PIM-DM are common in PIM-SM.

2.1.5.1.2 debug ipv6 pim timer srt

Command: debug ipv6 pim timer srt

no debug ipv6 pim timer srt

Function: Enable debug switch of PIM-DM state-refresh timer information in detail; the "**no debug ipv6 pim timer srt**" command disenables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: Enable the switch, and display PIM-DM state-refresh timer information in detail

Example: Switch # debug ipv6 pim timer srt

Remark: Other debug switches in PIM-DM are common in PIM-SM.

2.1.5.1.3 show ipv6 mroute

Command: show ipv6 mroute [<GroupAddr> [<SourceAddr>]]

Function: show IPv6 software multicast route table

Parameter: GroupAddr: show the multicast entries relative to this Group address.

SourceAddr：show the multicast route entries relative to this source address

Default: None

Command Mode：Admin mode and global mode

Usage Guide:

Example: show all entries of IPv6 multicast route table

Switch(config)# show ipv6 mroute

Name: Loopback, Index: 2002, State:49

Name: Vlan1, Index: 2006, State:1043

Name: Vlan11, Index: 2007, State:1043

Name: Vlan12, Index: 2008, State:1043

Name: Tunnel1, Index: 2009, State:d1

Name: Tunnel2, Index: 0, State:0

Name: pim6reg, Index: 2010, State:c1

Name: pimreg, Index: 2011, State:c1

The total matched ip6mr active mfc entries is 1, unresolved ip6mr entries is 1

Group	Origin	Iif	Wrong	Oif:TTL
ff2f::1	2014:1:2:3::2	Tunnel1	0	2008:1
ff3f::1	2012:1:2:3::2	NULL	4	0:0

Displayed information	Explanation
Name	the name of interface
Index	the index number of interface
State	the state of interface
The total matched ipmr active mfc entries	The total matched active IP multicast route mfc（multicast forwarding cache） entries
unresolved ipmr entries	unresolved ip multicast route entries
Group	the destination address of the entries
Origin	the source address of the entries
Iif	ingress interface of the entries
Wrong	packets received from the wrong interface
Oif	egress interface of the entries
TTL	the value of TTL

Remark: This command is common in PIM-SM6.

2.1.5.1.4 show ipv6 pim interface

Command: show ipv6 pim interface [detail|]

Function: Display PIM interface information

Parameter: None

Default: None

Command Mode: Any Mode

Example:

```
Switch#show ipv6 pim interface
Interface VIFindex Ver/     Nbr       DR
                           Mode     Count    Prior
Vlan2        0             v2/S     0          1
     Address           : fe80::203:fff:fee3:1244
     Global Address: 2000:1:111::100
     DR                : this system
Vlan3        2             v2/S     0          1
     Address           : fe80::203:fff:fee3:1244
     Global Address: 2000:10:1:13::1
     DR                : this system
```

Displayed Information	Explanations

Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count	The interface's neighbor count
DR Prior	Dr priority
DR	The interface's DR address

2.1.5.1.5 show ipv6 pim mroute dense-mode

Command: show ipv6 pim mroute dense-mode [group <*X:X::X:X*>] [source <*X:X::X:X*>]

Function: Display PIM-DM message forwarding items.

Parameter:group<X:X::X:X>: displays forwarding items relevant to this multicast address

Source < X:X::X:X >: displays forwarding items relevant to this source.

Default: Do not display

Command Mode: Admin Mode

Usage Guide: The command shows PIM-DM multicast forwarding items, namely forwarding items of forward multicast packet in system FIB table

Example: Display all of PIM-DM message forwarding items

Switch(config)#show ipv6 pim mroute dense-mode

IP Multicast Routing Table

(*,G) Entries: 1

(S,G) Entries: 1

(*, ff1e::15)

Local

(2000:10:1:12::11, ff1e::15)

RPF nbr: ::

RPF idx: Vlan12

Upstream State: FORWARDING

Origin State: ORIGINATOR

Local

Pruned

Asserted

Outgoing

Switch#

Displayed Information	Explanations
(*, ff1e::15)	(*,G) Forwaridng item
(2000:10:1:12::11, ff1e::15)	(S,G) Forwarding item

RPF nbr	Backward path neighbor, upstream neighbor of source direction in DM, 0.0.0.0 expresses the switch is the first hop.
RPF idx	Interface located in RPF neighbor
Upstream State	Upstream direction, including FORWARDING(forwarding upstream data), PRUNED(Upstream stops forwarding data), ACKPENDING(waiting for upstream response, forwarding upstream data)
Origin State	The two states: ORIGINATOR(on transmit state-refresh state), NON_ORIGINATOR(on non_transmit state-refresh state)
Local	Join Local position joins interface, the interface receives IGMP Join
Pruned	PIM prunes interface, the interface receives Prune messages
Asserted	Asserted state
Outgoing	Multicast data finally exported from interface is index number, index is 2 in this case. It can check interface information in detail by commanding show ip pim interface

2.1.5.1.6 show ipv6 pim neighbor

Command: show ipv6 pim neighbor [detail|]

Function: Display router neighbors

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display multicast router neighbors maintained by the PIM

Example:

Switch(config)#show ipv6 pim neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
Fe80::203:fff:fee3:1244	Vlan1	00:00:10/00:01:35	v2	1 /DR
fe80::20e:cff:fe01:facc	Vlan1	00:00:13/00:01:32	v2	1 /

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Neighbor interface
Uptime/Expires	Running time /overtime
Ver	Pim version ,v2 usually
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP

2.1.5.1.7 show ipv6 pim nexthop

Command: show ipv6 pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display the PIM buffered nexthop router information

Example:

Switch#show ipv6 pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable ….

Destination Type Nexthop

Nexthop ..Nexthop Nexthop Metric Pref Refcnt

Num Addr

Ifindex Name

2000:1:111::11 ..S. 1 :

: 2004 0 0 2

2000:1:111::100 .RS. 1 ::

2004 0 0 2

2004 0 0 2

Displayed Information	Explanations
Destination	Destination of next item
Type	N: created nexthop,RP direction and S direction are not determined . R: RP derection S: source direction U: can't reach
Nexthop Num	Nexthop number
Nexthop Addr	Nexthop address
Nexthop Ifindex	Nexthop interface index

Nexthop Name	Nexthop name
Metric	Metric Metric to nexthop
Pref	Preference Route preference
Refcnt	Reference count

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 bandwith 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.

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.

2.2.2 PIM-SM Configuration Task List

1、 Start PIM-SM (Required)

2、 To configure static multicast routing entries(required)

3、 Configure PIM-SM auxiliary parameters (Optional）

（1） Configure PIM-SM interface parameters

1) Configure PIM-SM hello message interval time
2) Configure interface as PIM-SM domain boundary
3) To configure the interface as the boundary interface of the PIM-SM6 protocol
4) To configure the interface as the management boundary of the PIM-SM6 protocol

（2） Configure PIM-SM global parameters

1) Configure switch as candidate BSR
2) Configure switch as candidate RP
3) Configure static RP

4、 Shut down PIM-SM Protocol

1. Start PIM-SM Protocol

It's easy to make basic configuration of the PIM-SM routing protocol in EDGECORE layer 3 switch, only need to turn on PIM multicast switch in Global Mode and turn on PIM-SM switch on relevant interface.

Command	**Explanation**
Global Mode	
[no] ipv6 pim multicast-routing	Enable PIM-SM Protocol on each interface (but below commands are required to really start PIM-SM protocol on the interface), and the NO operation of this command shuts PIM-SM Protocol on all interfaces. (Required)

And then turn on PIM-SM switch on the interface

Command	**Explanation**
Port Configuration Mode	
[no] ipv6 pim sparse-mode [passive]	Start PIM-SM Protocol of the interface. The NO operation of this command shuts the PIM-SM Protocol of this interface. (Required)

2．To configure static multicast routing entries

Command	Notes
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 PIM-SM Auxiliary Parameters

（1）Configure PIM-SM Interface Parameters

1）Configure PIM-SM hello message interval time

Command	**Explanation**
Port Configuration Mode	
Ipv6 pim hello-interval < *interval*> **no ipv6 pim hello-interval**	Configure interface PIM-SM hello message interval time; the NO operation of this command restores the default value.

2）Configure PIM-SM hello message holdtime

Command	**Explanation**
Port Configuration Mode	
Ipv6 pim hello-holdtime <*value*> **no ipv6 pim hello-holdtime**	Configure the value of holdtime domain in interface PIM-SM hello message; the NO operation of this command restores the default value.

3）Configure PIM-SM Neighbor Access-list

Command	**Explanation**
Port Configuration Mode	
(no)ipv6 pim neighbor-filter <a*ccess-list-name*>	Configure Neighbor Access-list. If a neighbor is filtered by the list and a connection has been set up with this neighbor, then this connection will be cut off immediately; and if no connection is set up yet, then this connection can’t be created.

4）To configure the interface as the boundary interface of the PIM-SM6 protocol

Command	Notes
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）To configure the interface as the management boundary of the PIM-SM6 protocol

Command	Notes
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 PIM-SM Global Parameters

1）Configure switch to be candidate BSR

Command	**Explanation**
Global Mode	
Ipv6 pim bsr-candidate <*ifname*> **[*hash-mask-length*] [*priority*]** **no ipv6 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 BSRs. The NO operation is to cancel the configuration of BSR.

2）Configure switch to be candidate RP

Command	**Explanation**
Global Mode	

Ipv6 pim rp-candidate <*ifname*> [<*group range*>] [<*priority*>] **(no) ipv6 pim rp-candidate <*ifname*>**	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 RPs. The NO operation is to cancel the configuration of RP.

3）Configure Static RP

Command	**Explanation**
Global Mode	
Ipv6 pim rp-address <*rp-address*> [<*group-range*>] **no ipv6 pim rp-address <*rp-address*> {all|<*group-range*>}**	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 RPs. The NO operation is to cancel the configuration of RP.

4. Shut down PIM-SM Protocol

Command	**Explanation**
Port Configuration Mode	
no ipv6 pim sparse-mode	Shut down PIM-SM Protocol.
Global Mode	
no ipv6 pim multicast-routing	Shut down PIM-SM Protocol globally.

2.2.3 Command for PIM-SM

2.2.3.1 ipv6 mroute

Command: 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*>]

Function: To configure static multicast entry. The no command is to delete some static multicast entries or some egress interfaces.

Parameter: <X:X::X:X> <X:X::X:X> are the source address and group address of multicast. <ifname>, the first one is ingress interface, follow is egress interface.

Command Mode: Global Mode

Default: None.

Usage Guide: The <ifname> should be valid VLAN interfaces. The multicast data flow will not be forwarded unless PIM is configured on the egress interface and the interface is UP. If the state of the interface is not UP, or PIM is not configured, or RPF is not valid, the multicast data flow will not be fordwarded.

Example:

Switch(config)#ipv6 mroute 2001::1 ff1e::1 v10 v20 v30

Switch(config)#

2.2.3.2 ipv6 pim accept-register

Command: ipv6 pim accept-register list <a*cess-list-name*>

no ipv6 pim accept-register

Function: Filter the specified multicast group.

Parameter: <a*cess-list-name*> is the applying access-list name

Default: Permit the multicast registers from any sources to any groups

Command Mode: Global Mode

Usage Guide: This command is used to configure the access-list filtering the PIM REGISTER packets.The addresses of the access-list respectively indicate the filtered multicast sources and multicast groups' information. For the source-group combinations that match DENY ,PIM sends REGISTER-STOP immediately and does not create group records when receiving REGISTER packets.Unlike other access-list,when the access-list is configured ,the default value is PERMIT..

Example: Configure the filtered register message's rule to myfilter.

Switch(config)#ipv6 pim accept-register list myfilter

Switch(config)#ipv6 access-list standard myfilter

Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::10/128

2.2.3.3 ipv6 pim bsr-border

Command: ipv6 pim bsr-border

no ipv6 pim bsr-border

Function: To configure or delete PIM6 BSR-BORDER interface.

Parameter: None

Default: Non-BSR-BORDER

Command Mode: Interface Configuration Mode.

Usage Guide: To configure the interface as the BSR-BORDER. If configured, BSR related messages will not received from or sent to the specified interface. All the networks connected to the interface will be considered as directly connected.

Example:

Switch(Config-if-Vlan1)#ipv6 pim bsr-border

Switch(Config-if-Vlan1)#

2.2.3.4 ipv6 pim bsr-candidate

Command: ipv6 pim bsr-candidate <*ifname*> [<*hash-mask-length*>] [<*priority*>]

no ipv6 pim bsr-candidate [*ifname*]

Function: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. The command **"no ipv6 pim bsr-candidate [*ifname*]"** command disables the candidate BSR.

Parameter: <*ifname*> is the specified interface name;

[*hash-mask-length*] is the specified hash mask length.It's used for the RP enable selection and ranges from 0 to 32.;

[*priority*] is the candidate BSR priority and ranges from 0 to 255. If this parameter is not configured ,the default priority value is 0

Default: This switch is not a candidate BSR router

Command Mode: Global Mode

Usage Guide: This command is the candidate BSR configure command in global mode and is used to configure PIM-SM information about candidate BSR in order to compete the BSR router with other candidate BSRs. Only this command is configured , this switch is the BSR candidate router.

Example: Globally configure the interface vlan1 as the candidate BSR-message transmitting interface.

Switch (config)# ipv6 pim bsr-candidate vlan1 30 10

2.2.3.5 ipv6 pim cisco-register-checksum

Command:ipv6 pim cisco-register-checksum [group-list <*access-list name*>]

no ipv6 pim cisco-register-checksum [group-list <*access-list name*>]

Function: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.

Default: Compute the checksum according to the regester packets's head length default: 8

Parameter: <*access-list name*> is the applying simple access-list.

Command Mode: Global Mode

Usage Guide: This command is uesd to interact with older Cisco IOS version.

Example: Configure the register packet's ckecksum of the group specified by myfilter to use the whole packet's length.

Switch(config)#ipv6 pim cisco-register-checksum group-list myfilter

Switch(config)#ipv6 access-list standard myfilter

Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::10/128

2.2.3.6 ipv6 pim dr-priority

Command: ipv6 pim dr-priority <*priority*>

no ipv6 pim dr-priority

Function: Configure, disable or change the interface's DR priority. The neighboring nodes in the same net segment select the DR in their net segment according to hello packets. The "**no ipv6 pim dr-priority**" command restores the default value

Parameter: <*priority*> priority,it ranges from 0 to 4294967294

Default: 1

Command Mode: Interface Configuration Mode

Usage Guide: Range from 0 to 4294967294, the higher value has more priority. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Switch (config)# interface vlan 1

Switch(Config-if-Vlan1)ipv6 pim dr-priority 100

2.2.3.7 ipv6 pim exclude-genid

Command: **ipv6 pim exclude-genid**

no ipv6 pim exclude-genid

Function: This command makes the Hello packets sent by PIM SM do not include GenId option, the "**no ipv6 pim exclude-genid**" command restores the default value

Parameter: None

Default: The Hello packets include GenId option.

Command Mode: Interface Configuration Mode

Usage Guide: This command is used to interact with older Cisco IOS version. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure the Hello packets sent by the switch do not include GenId option

Switch(Config-if-Vlan1)#ipv6 pim exclude-genid

2.2.3.8 ipv6 pim hello-holdtime

Command: ipv6 pim hello-holdtime <*value*>

no ipv6 pim hello-holdtime

Function: Configure or disable the Holdtime option in the Hello packets,this value is to describe neighbore holdtime,if the switch hasn't received the neighbore hello packets when the holdtime is over, this neighbore is deleted.

Parameter: <*value*> is the value of holdtime.

Default: The default value of Holdtime is 3.5*Hello_interval, Hello_interval's default value is

30s,so Holdtime's default value is 105s.

Command Mode: Interface Configuration Mode

Usage Guide: If this value is not configured, hellotime's default value is 3.5*Hello_interval. If the configured holdtime is less than the current hello_interval , this configuration is denyed. Every time hello_interval is updated, the Hello_holdtime will update according to the following rules: If hello_holdtime is not configured or hello_holdtime is configured but less than current hello_interval,hello_holdtime is modified to 3.5*hello_interval, otherwise the configured value is maintained. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure vlan1's Hello Holdtime to 10s

Switch (config)# interface vlan1

Switch (Config -if-Vlan1)#ipv6 pim hello-holdtime 10

2.2.3.9 ipv6 pim hello-interval

Command: ipv6 pim hello-interval <*interval*>

no ipv6 pim hello-interval

Function: Configure the interface's hello_interval of pim hello packets. The "**no ipv6 pim hello-interval**" command restores the default value.

Parameter: <*interval*> is the hello_interval of periodically transmitted pim hello packets', ranges from 1 to 18724s

Default: The default periodically transmitted pim hello packets' hello_interval is30s.

Command Mode: Interface Configuration Mode

Usage Guide: Hello messages make pim switches oriente each other and determine neighbore relationship. Pim switch annouce the existance of itself by periodically transmitting hello messages to neighbores. If no hello messages from neighores are received in the certain time, the neighbore is considered lost. This value can't be greater than neighbore overtime. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure vlan's pim-sm hello_interval.

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 pim hello-interval 20

2.2.3.10 ipv6 pim ignore-rp-set-priority

Command: ipv6 pim ignore-rp-set-priority

no ipv6 pim ignore-rp-set-priority

Function: When RP selection is carried out, this command configures the switch to enable Hashing regulation and ignore RP priority. This command is used to interact with older Cisco IOS versions.

Default: None

Parameter: None

Command Mode: Global Mode

Usage Guide: When selecting RP, Pim usually will select according to RP priority. When this command is configured, pim will not select according to RP priority. Unless there are older routers in the net, this command is not recommended.

Example: Configure to ignore RP priority.

Switch(config)#ipv6 pim ignore-rp-set-priority

2.2.3.11 ipv6 pim jp-timer

Command: ipv6 pim jp-timer <*value*>

no ipv6 pim jp-timer

Function: Configure to add JP timer. **no ipv6 pim jp-timer** restores the default value.

Parameter: <*value*> ranges from 10 to 65535

Default: 60s

Command Mode: Global Mode

Usage Guide: Configure the interval of tnansmitting J/P messages to59s.

Example: Switch(config)#ipv6 pim jp-timer 59

2.2.3.12 ipv6 pim multicast-routing

Command: ipv6 pim multicast-routing

no ipv6 pim multicast-routing

Function: Enable PIM-SM globally. The "**no ipv6 pim multicast-routing**" command disables PIM-SM globally.

Parameter: None

Default: Disabled PIM-SM protocol

Command Mode: Global Mode

Usage Guide: Inspect the changing information about pim state by this switch..

Example: Enable PIM-SM globally.

Switch (config)#ipv6 pim multicast-routing

2.2.3.13 ipv6 pim neighbor-filter

Command: ipv6 pim neighbor-filter <a*cess-list-name*>

no ipv6 pim neighbor-filter <a*cess-list-name*>

Function: Configure the neighbore access-list. If filtered by the lists and connections with neighbors are created, this connections are cut off immediately. If no connection is created, this conncetion can't be created.

Parameter: <*acess-list-name*> is the applying access-list' name

Default: No neighbor filter configuration

Command Mode: Interface Configuration Mode

Usage Guide: ACL's default is DENY. If configuring access-list 1,access-list 1's default is deny. In the following example,if "permit any-source" is not configured, deny fe80:20e:cff:fe01:facc is the same as deny any-source. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Configure vlan's pim neighbore access-list

Switch (Config-if-Vlan1)#ipv6 pim neighbor-filter myfilter

Switch(config)#ipv6 access-list standard myfilter

Switch(config_IPv6_Std-Nacl-myfilter)#deny fe80:20e:cff:fe01:facc

Switch(config)#ipv6 access-list standard myfilter

Switch(config_IPv6_Std-Nacl-myfilter)#permit any

2.2.3.14 ipv6 pim register-rate-limit

Command: ipv6 pim Register-rate-limit <*limit*>

no ipv6 pim Register-rate-limit

Function: This command is used to configure the speedrate of DR sending register packets, the unit is packet/second. the "**no ipv6 pim Register-rate-limit**" command restores the default value. This configured speedrate is each（S, G）state's, not the whole systems.

Parameter: <*limit*> ranges from 1 to 65535

Default: No limit for sending speed

Command Mode: Golbal Mode

Usage Guide: Configure the speedrate of DR sending register packets

Example: Configure the speedrate of DR sending register packets to 59 p/s

Switch(config)#ipv6 pim Register-rate-limit 59

2.2.3.15 ipv6 pim register-rp-reachability

Command: ipv6 pim Register-rp-reachability

no ipv6 pim Register-rp-reachability

Function: This command makes DR check the RP reachability in the process of registration

Parameter: None

Default: Do not check

Command Mode: Global Mode

Usage Guide: This command configures DR whether or not to check the RP reachability.

Example: Configure the router to check the RP reachability before sending register packets.

Switch(config)# ipv6 pim Register-rp-reachability

2.2.3.16 ipv6 pim register-source

Command: ipv6 pim register-source {<*source-address*> |<*ifname*>|vlan <*vlan-id*>}

no ipv6 pim register-source

Function: This command is to configure the source address of register packets sent by DR to overwrite default source address. This default source address is uaually the RPF neighbor of source host direction.

Parameter: *<ifname>* is the interface name that will be the register packets source.

<source-address> is the interface address will be the register packets source. In the format of hex without prefix length.

<vlan-id> is the VLAN ID.

Default: Do not check.

Command Mode: Global Mode

Usage Guide: The "**no ipv6 pim register-source**" command restores the default value,no more parameter is needed. Configured address must be reachable to Register-Stop messages sent by RP. It's usually a circle address, but it can be other physical addresses. This address must be announcable through unicast router protocols of DR.

Example: Configure the source address of the sent register packets to vlan1's address

Switch(config)# ipv6 pim register-source Vlan1

2.2.3.17 ipv6 pim register-suppression

Command: ipv6 pim register-suppression <***value***>

no ipv6 pim register-suppression

Function: This command is to configure the value of register suppression timer,the unit is second

Parameter: <***value***> is the timer's value,it ranges from 10 to 65535s

Default: 60s

Command Mode: Global Mode

Usage Guide: If this value is configured at DR,it's the value of register suppression timer; if this value is configured at RP and ipv6 pim rp-register-kat is not used at RP, this command modifies Keepalive-period value. The "**no ipv6 pim register-suppression**" command restores the default value.

Example: Configure the value of register suppression timer to 30s

Switch(config)# ipv6 pim register-suppression 30

2.2.3.18 ipv6 pim rp-address

Command: ipv6 pim rp-address <*rp-address*> [<*group-range*>]

no ipv6 pim rp-address <*rp-address*> [all|<*group-range*>]

Function: This command is to configure static RP globally or in a multicast address range. The "**no ipv6 pim rp-address**" command cancels static RP.

Parameter: <*rp-address*> is the RP address, the format is **X:X::X:X** ,**ipv6** address

<*group-range*> is the expected RP, the format is **X:X::X:X/M, ipv6** address and prefix length

all:all the ranges

Default: This switch is not a RP static router

Command Mode: Global Mode

Usage Guide: This command is to configure static RP globally or in a multicast address range.

Example: Configure 2000:112::8 as RP address globally

Switch (config)# ipv6 pim rp-address 2000:112::8 ff1e::/64

2.2.3.19 ipv6 pim rp-candidate

Command: Ipv6 pim rp-candiate <*ifname*> [<*group range*>] [<*priority*>]

no ipv6 pim rp-candiate

Function: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs.The **"no ipv6 pim rp-candiate**" command cancels the candidate RP.

Parameter: <*ifname*> is the name of the interface;

<*group range*> is the group range of the candidate RP,the format is **X:X::X:X/M**, **ipv6** address and prefix length;

<*priority*> is the RP selection priority, ranges from 0 to 255, the default value is 192, the lower value has more priority

Default: This switch is not a RP static router.

Command Mode: Gobal Mode

Usage Guide: This command is the candidate RP global configure command, it is used to configure PIM-SM candidate RP information in order to compete RP router with other candidate RPs.Only this command is configured,this switch is the RP candidate router

Example: Configure vlan1 as the sending interface of candidate RP announce messages

Switch (config)# ipv6 pim rp-candidate vlan1 100

2.2.3.20 ipv6 pim rp-register-kat

Command: ipv6 pim rp-register-kat <*vaule*>

no ipv6 pim rp-register-kat

Function: This command is to congifure the KAT(KeepAlive Timer)value of the RP(S,G)items,the unit is second. The "**no ipv6 pim rp-register-kat**" comannd restores the default value

Parameter: <*vaule*> is the timer value,ranges from 1 to 65535s

Default: 185s

Command Mode: Global Mode

Usage Guide: Configure rp-register-kat interval to 30s

Example: Switch(config)# ipv6 pim rp-register-kat 30

2.2.3.21 ipv6 pim scope-border

Command: ipv6 pim scope-border [<*500-599*>|<*acl_name*>]

no ipv6 pim scope-border

Function: To configure or delete management border of PIM6.

Parameters: <1-99> is the ACL number for the management border.

<acl_name> is the ACL name for the management border.

Default: Not management border. If no ACL is specified, the default management border will be used.

Command Mode: Interface Configuration Mode

Usage Guide: To configure the management border and the ACL for the PIM protocol. The multicast data flow will not be forwarded to the SCOPE-BORDER.

Example:

Switch(Config-if-Vlan2)#ipv6 pim scope-border 503

Switch(Config-if-Vlan2)#

2.2.3.22 ipv6 pim sparse-mode

Command: ipv6 pim sparse-mode [passive]

no ipv6 pim sparse-mode [passive]

Function: Enable PIM-SM on the interface. **no ipv6 pim sparse-mode [passive]** disables PIM-SM.

Parameter: [*passive*] means to disable PIM-SM (that's PIM-SM doesn't receive any packets) and only enable MLD(reveice and transmit MLD packets).

Default: Disabled PIM-SM

Command Mode: Interface Configuration Mode

Usage Guide: Enable PIM-SM on the interface. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.

Example: Enable PIM-SM on the interface vlan1

Switch (config)#interface vlan 1

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

2.2.3.23 ipv6 pim ssm

Command: ipv6 pim ssm {default|range <*access-list-name* >}

no ipv6 pim ssm

Function: Configure the range of pim ssm multicast address. The "**no ipv6 pim ssm**" command deletes configured pim ssm multicast group.

Parameter: ***default :*** indicates the default range of pim ssm multicast group is ff3x::/32.

<access-list-number > is the name of applying access-list.

Default: Do not configure the range of pim ssm group address

Command Mode: Global Mode

Usage Guide:

1. Only this command is configured, pim ssm can be available.

2. Before configuring this command, make sure ipv6 pim multicasting succeed.

3. Access-list only can use the lists created by ipv6 access-list.

4.Users can execute this command first and then configure the corresponding acl; or delete corresponding acl in the bondage. After the bondage, only command no ipv6 pim ssm can release the bondage.

5 .If ssm is needed, this command should be configured at the related edge route. For example, the local switch with igmp(must) and multicast source DR or RP(at least one of the two) configure this command, the middle switch need only enable PIM-SM.

Example: Configure the switch to enable PIM-SSM, the group's range is what is specified by access-list 23.

```
Switch (config)#ipv6 pim ssm range 23
Switch(config)#ipv6 access-list standard myfilter
Switch(config_IPv6_Std-Nacl-myfilter)#permit ff1e::/48
```

2.2.4 PIM-SM 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.

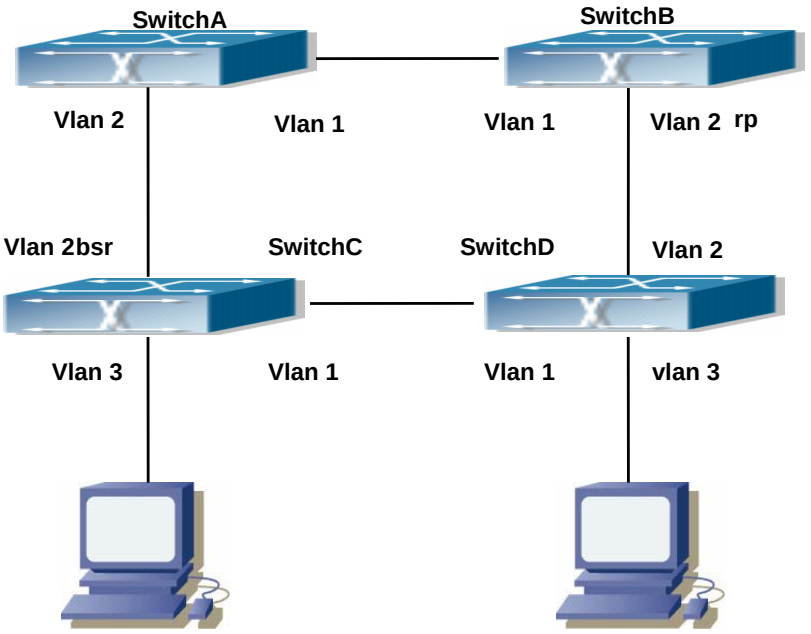


Fig 2-2 PIM-SM Typical Environment

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

2.2.5 PIM-SM Troubleshooting Help

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.

2.2.5.1 Monitor and debug command

2.2.5.1.1 debug ipv6 pim events

Command: debug ipv6 pim events

no debug ipv6 pim events

Function: Enable or Disable pim events debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable “pim events debug” switch and display events information about pim operation.

Example: Switch# debug ipv6 pim events

2.2.5.1.2 debug ipv6 pim mfc

Command: debug ipv6 pim mfc（in|out|）

no debug ipv6 pim mfc（in|out|）

Function: Enable or Disable pim mfc debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable pim mfc debug switch and display generated and transmitted multicast id’s information.

Example: Switch# debug ipv6 pim mfc in

2.2.5.1.3 debug ipv6 pim mib

Command: debug ipv6 pim mib

no ipv6 debug pim mib

Function: Enable or Disable PIM MIB debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect PIM MIB information by PIM MIB debug switch. It’s not available now and

it’s for the future extension.

Example: Switch# debug ipv6 pim mib

2.2.5.1.4 debug ipv6 pim nexthop

Command: debug ipv6 pim nexthop

no debug ipv6 pim nexthop

Function: Enable or Disable pim nexthop debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect PIM NEXTHOP changing information by the pim nexthop switch.

Example: Switch# debug ipv6 pim nexthop

2.2.5.1.5 debug ipv6 pim nsm

Command: debug ipv6 pim nsm

no debug ipv6 pim nsm

Function: Enable or Disable pim debug switch communicating with Network Services

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the communicating information between pim and Network Services by this switch.

Example: Switch# debug ipv6 pim nsm

2.2.5.1.6 debug ipv6 pim packet

Command: debug ipv6 pim packet [in|out|]

no debug ipv6 pim packet [in|out|]

Function: Enable or Disable pim debug switch

Parameter: in display only received pim packets

out display only transmitted pim packets

none display both

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the received and transmitted pim packets by this switch.

Example: Switch# debug ipv6 pim packet in

2.2.5.1.7 debug ipv6 pim state

Command: debug ipv6 pim state

no debug ipv6 pim state

Function: Enable or Disable pim debug switch

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Inspect the changing information about pim state by this switch.

Example: Switch# debug ipv6 pim state

2.2.5.1.8 debug ipv6 pim timer

Command:debug ipv6 pim timer

debug ipv6 pim timer assert

debug ipv6 pim timer assert at

debug ipv6 pim timer bsr bst

debug ipv6 pim timer bsr crp

debug ipv6 pim timer bsr

debug ipv6 pim timer hello ht

debug ipv6 pim timer hello nlt

debug ipv6 pim timer hello tht

debug ipv6 pim timer hello

debug ipv6 pim timer joinprune et

debug ipv6 pim timer joinprune grt

debug ipv6 pim timer joinprune jt

debug ipv6 pim timer joinprune kat

debug ipv6 pim timer joinprune ot

debug ipv6 pim timer joinprune plt

debug ipv6 pim timer joinprune ppt

debug ipv6 pim timer joinprune pt

debug ipv6 pim timer joinprune

debug ipv6 pim timer register rst

debug ipv6 pim timer register

no debug ipv6 pim timer

no debug ipv6 pim timer assert

no debug ipv6 pim timer assert at

no debug ipv6 pim timer bsr bst

no debug ipv6 pim timer bsr crp

no debug ipv6 pim timer bsr

no debug ipv6 pim timer hello ht

no debug ipv6 pim timer hello nlt

no debug ipv6 pim timer hello tht

no debug ipv6 pim timer hello

no debug ipv6 pim timer joinprune et

no debug ipv6 pim timer joinprune grt

no debug ipv6 pim timer joinprune jt

no debug ipv6 pim timer joinprune kat

no debug ipv6 pim timer joinprune ot

no debug ipv6 pim timer joinprune plt

no debug ipv6 pim timer joinprune ppt

no debug ipv6 pim timer joinprune pt

no debug ipv6 pim timer joinprune

no debug ipv6 pim timer register rst

no debug ipv6 pim timer register

no debug ipv6 pim timer

Function: Enable or Disable each pim timer

Parameter: None

Default: Disabled

Command Mode: Admin Mode.

Usage Guide: Enable the specified timer's debug information

Example: Switch# debug ipv6 pim timer assert

2.2.5.1.9 show ipv6 pim bsr-router

Command: show ipv6 pim bsr-router

Function: Display BSR address

Parameter: None

Default: None

Command Mode: Admin Mode.

Example:

Switch#show ipv6 pim bsr-router

PIMv2 Bootstrap information

This system is the Bootstrap Router (BSR)

BSR address: 2000:1:111::100 (?)

Uptime: 00:16:00, BSR Priority: 0, Hash mask length: 126

Next bootstrap message in 00:00:10

Role: Candidate BSR

State: Elected BSR

Next Cand_RP_advertisement in 00:00:10

RP: 2000:1:111::100(Vlan2)

Displayed Information	Explanations
BSR address	Bsr-router Address
Priority	Bsr-router Priority
Hash mask length	Bsr-router hash mask length

State	The current state of this candidate BSR, Elected BSR is selected BSR

2.2.5.1.10 show ipv6 pim interface

Command: show ipv6 pim interface [detail]

Function: Display PIM interface information

Parameter: None

Default: None

Command Mode: Any Mode

Example:

```
Switch#show ipv6 pim interface
Interface VIFindex Ver/     Nbr       DR
                           Mode     Count    Prior
Vlan2        0             v2/S     0         1
     Address           : fe80::203:fff:fee3:1244
     Global Address: 2000:1:111::100
     DR                : this system
Vlan3        2             v2/S     0         1
     Address           : fe80::203:fff:fee3:1244
     Global Address: 2000:10:1:13::1
     DR                : this system
```

Displayed Information	Explanations
Address	Interface address
Interface	Interface name
VIF index	Interface index
Ver/Mode	Pim version and mode,usually v2,sparse mode displays S,dense mode displays D
Nbr Count	The interface's neighbor count
DR Prior	Dr priority
DR	The interface's DR address

2.2.5.1.11 show ipv6 pim mroute sparse-mode

Command: show ipv6 pim mroute sparse-mode

Function: Display the multicast route table of PIM-SM

Parameter: None

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: Display the BSP routers in the network maintained by PIM-SM

Example:

Switch#show ipv6 pim mr group ff1e::15
IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0
(*, ff1e::15)
RP: 2000:1:111::100
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
Local
Joined
Asserted
FCR:
(2000:1:111::11, ff1e::15)
RPF nbr: ::
RPF idx: None
SPT bit: 1
Upstream State: JOINED
Local .
Joined
Asserted
Outgoing
(2000:1:111::11, ff1e::15, rpt)
RP: 2000:1:111::100
RPF nbr: ::
RPF idx: None
Upstream State: NOT PRUNED
Pruned
Outgoing

Displayed Information	Explanations
Entries	The counts of each item
RP	Share tree's RP address
RPF nbr	RP direction or upneighbor of source direction

RPF idx	RPF nbr interface
Upstream State	Upstream State,there are two state of Joined(join the tree,expect to receive data from upstream) and Not Joined(quit the tree,not expect to receive data from upstream), and more options such as RPT Not Joined, Pruned, Not Pruned are available for（S,G,rpt.）
Local	Local join interface, this interface receive IGMPJoin
Joined	PIM join interfacce, this interface receive J/P messages
Asserted	Asserted state
Outgoing	Final outgoing of multicast data

2.2.5.1.12 show ipv6 pim neighbor

Command: show ipv6 pim neighbor [detail]

Function: Display router neighbors

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display multicast router neighbors maintained by the PIM

Example:

Switch(config)#show ipv6 pim neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
Fe80::203:fff:fee3:1244	Vlan1	00:00:10/00:01:35	v2	1 /DR
fe80::20e:cff:fe01:facc	Vlan1	00:00:13/00:01:32	v2	1 /

Displayed Information	Explanations
Neighbor Address	Neighbor address
Interface	Neighbor interface
Uptime/Expires	Running time /overtime
Ver	Pim version ,v2 usually
DR Priority/Mode	DR priority in the hello messages from the neighbor and if the neighbor is the interface's DP

2.2.5.1.13 show ipv6 pim nexthop

Command: show ipv6 pim nexthop

Function: Display the PIM buffered nexthop router in the unicast route table

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display the PIM buffered nexthop router information

Example:

Switch#show ipv6 pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable ….

Destination Type Nexthop

Nexthop ..Nexthop Nexthop Metric Pref Refcnt

Num Addr

Ifindex Name

2000:1:111::11 ..S. 1 :

: 2004 0 0 2

2000:1:111::100 .RS. 1 ::

2004 0 0 2

2004 0 0 2

Displayed Information	Explanations
Destination	Destination of next item
Type	N: created nexthop,RP direction and S direction are not determined . R: RP derection S: source direction U: can't reach
Nexthop Num	Nexthop number
Nexthop Addr	Nexthop address
Nexthop Ifindex	Nexthop interface index
Nexthop Name	Nexthop name
Metric	Metric Metric to nexthop
Pref	Preference Route preference
Refcnt	Reference count

2.2.5.1.14 show ipv6 pim rp-hash

Command: show ipv6 pim rp-hash X:X::X:X

Function: Display the RP address of group X:X::X:X's merge point

Parameter: Group address

Default: None

Command Mode: Any Mode

Usage Guide: Display the RP address corresponding to the specified group address

Example:

Switch#show ipv6 pim rp-hash ff1e::15

RP: 2000:1:111::100

Info source: 2000:1:111::100, via bootstrap

Displayed Information	Explanations
RP	Queried group'sRP
Info source	Bootstrap The source of Bootstrap information

2.2.5.1.15 show ipv6 pim rp mapping

Command: show ipv6 pim rp mapping

Function: Display Group-to-RP Mapping and RP

Parameter: None

Default: None

Command Mode: Any Mode

Usage Guide: Display the current RP and mapping relationship

Example:

Switch#show ipv6 pim rp mapping

PIM Group-to-RP Mappings

This system is the Bootstrap Router (v2)

Group(s): ff00::/8

RP: 2000:1:111::100

Info source: 2000:1:111::100, via bootstrap, priority 192

Uptime: 00:10:24, expires: 00:02:06

Group(s): ff00::/8, Static

RP: 2000:1:111::100

Uptime: 00:11:01

Displayed Information	Explanations
Group(s)	Group address range of RP
Info source	Source of Bootstrap messages
Priority	Priority of Bootstrap messages

2.3 ANYCAST RPv6 Configuration

2.3.1 ANYCAST RPv6 Introduction

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 RPs will cause a new problem that is if the multicast source and the receivers are registered to different RPs, 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 RPs, Anycast RP defines that the nearest RP to the multicast source should forward the source register messages to all the other RPs to guarantee that all joiners of the RPs 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 RPv6 Configuration Task

1. Enable ANYCAST RPv6 function
2. Configure ANYCAST RPv6

1. Enable ANYCAST RPv6 function

Command	Explanation
Global configuration mode	
ipv6 pim anycast-rp **no ipv6 pim anycast-rp**	Enable ANYCAST RP function. (In order to actually enable the ANYCAST RP protocol, the following command is needed). (necessary) No operation will globally disable the ANYCAST RP function.

2. Configure ANYCAST RPv6

(1) Configure RP candidate

Command	Explanation
Global configuration mode	
ipv6 pim rp-candidate {vlan<*vlan-id*> | loopback<*index*> | <*ifname*>} [<*A:B::C:D*>][<*priority*>] **no ipv6 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 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 RPs.(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 RPs 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 RPs 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 RPs 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 the other-rp-addresses of other RPs communicating with it. This unicast address identifies other RPs and is used in the communication with local routers. The effect of **other-rp-address** refers to 2 respects: 1 Once this router (as a RP) receives the register message from a DR unicast, it should forward it to other RPs in the network to notify all the RPs 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 RPs one by one. No operation will cancel an other-rp-address communicating with this router.

2.3.3 ANYCAST RPv6 Configuration Commands

2.3.3.1 debug ipv6 pim anycast-rp

Command：debug ipv6 pim anycast-rp

no debug ipv6 pim anycast-rp

Function：Enable the debug switch of ANYCAST RP function; the no operation of this command will disable this debug switch.

Command Mode：Admin mode.

Default：The debug switch of ANYCAST RP is disabled by default.

Usage Guide：This command is used to enable the debug switch of ANYCAST RP of the router, it can display the information of handling PIM register packet of the switch——packet, and the information of events——event.

Example：

Switch#debug ipv6 pim anycast-rp

2.3.3.2 ipv6 pim anycast-rp

Command：**ipv6 pim anycast-rp**

no ipv6 pim anycast-rp

Function：Enable the ANYCAST RP of the switch; the no operation of this command is to disable the ANYCAST RP function.

Command Mode：Global configuration mode.

Default：The switch will not enable the ANYCAST RP by default.

Usage Guide：This command will globally enable ANYCAST RP protocol, but, in order to make ANYCAST RP work, it is necessary to configure self-rp-address and other-rp-address set.

Example：Enable ANYCAST RP in global configuration mode.

Switch(config)#ipv6 pim anycast-rp

2.3.3.3 ipv6 pim anycast-rp

Command：**ipv6 pim anycast-rp *<anycast-rp-addr> <other-rp-addr>***

no ipv6 pim anycast-rp *<anycast-rp-addr> <other-rp-addr>*

Function：Configure ANYCAST RP address（ARA）and the unicast addresses of other RPs communicating with this router(as a RP). The no operation of this command will cancel the unicast address of another RP in accordance with the configured RP address.

Parameters：***anycast-rp-addr***：RP address, the current absence of the candidate interface in accordance with the address is allowed

other-rp-addr：the unicast address of other RP communicating with this router(as a RP)

Command Mode: Global configuration mode.

Default：There is no configuration by default.

Usage Guide：

1 The anycast-rp-addr configured on this router(as a RP) is actually the RP address configured on multiple RPs in the network, in accordance with the address of RP candidate interface (or Loopback interface). The current absence of the candidate interface in accordance with the address is allowed when configuring.

2 Configure the other-rp-address of other RPs communicating with this router(as a RP). The unicast address identifies other RPs, and is used to communicate with the local router.

3 Once this router (as a RP) receives the register message from a DR unicast, it should forward it to other RPs in the network to notify all the RPs 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.

4 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 RPs one by one.

Example：Configure other-rp-address in global configuration mode.

Switch(config)#ipv6 pim anycast-rp 2000::1 2004::2

2.3.3.4 ipv6 pim anycast-rp self-rp-address

Command：**ipv6 pim anycast-rp self-rp-address <self-rp-addr>**

no ipv6 pim anycast-rp self-rp-address

Function：Configure the self-rp-address of this router(as a RP). This address will be used to exclusively identify this router from other RPs, and to communicate with other RPs. The no operation of this command will cancel the configured unicast address used by this router (as a RP) to communicate with other RPs.

Parameters：***self-rp-addr***：the unicast address used by this router (as a RP) to communicate with other RPs.

Command Mode：Global configuration mode.

Default：No self-rp-address is configured by default.

Usage Guide：

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 RPs 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.

3 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.

Example：Configure the self-rp-address of this router in global configuration mode.

Switch(config)#ipv6 pim anycast-rp self-rp-address 2000::1

2.3.3.5 ipv6 pim rp-candidate

Command ： ipv6 pim rp-candidate {vlan<*vlan-id*> |loopback<*index*> |<*ifname*>} [<*A:B::C:D*>] [<*priority*>]

no ipv6 pim rp-candidate

Function：Add a Loopback interface as a RP candidate interface based on the original PIM6-SM command; the no operation of this command is to cancel the Loopback interface as a RP candidate interface.

Parameters：***index***：Loopback interface index, whose range is <1-1024>

***vlan-id*:** the Vlan ID

***ifname*:** the specified name of the interface;

A:B::C:D/M: the ip prefix and mask

***<priority>*:** the priority of RP election, ranging from 0 to 255, the default value is 192. The smaller the value is the higher the priority is.

Command Mode：Global configuration mode.

Default Setting：No RP interface is configured by default.

Usage Guide：In order to support ANYCAST RP function, new rule allows configuring a Loopback interface to be the RP candidate interface. The RP candidate interface should be currently unique, and the address of which should be added into the router to make sure that PIM router can find the nearest RP. The “no ipv6 pim rp-candidate” command can be used to cancel the RP candidate.

Example：Configure Loopback1 interface as the RP candidate interface in global configuration mode.

Switch(config)#ipv6 pim rp-candidate loopback1

2.3.3.6 show debugging ipv6 pim

Command：**show debugging ipv6 pim**

Command Mode：Admin mode.

Usage Guide：The current state of anycast rp debug switch.

Example：

Switch(config)#show debugging ipv6 pim

Debugging status:

PIM anycast-rp debugging is on

2.3.3.7 show ipv6 pim anycast-rp first-hop

Command：**show ipv6 pim anycast-rp first-hop**

Command Mode：Admin mode.

Usage Guide：Display the state information of anycast rp, and display the mrt node information generated in the first hop RP which is currently maintained by the protocol.

Example：

Switch(config)#show ipv6 pim anycast-rp first-hop

IP Multicast Routing Table

(*,G) Entries: 0
(S,G) Entries: 1
(E,G) Entries: 0

INCLUDE (2000:1:111::2, ff1e::1)
Local .l.....

Display	Explanation
Entries	The number of all kinds of entries
INCLUDE	The information of mrt generated in the first hop RP

2.3.3.8 show ipv6 pim anycast-rp non-first-hop

Command：show ipv6 pim anycast-rp non-first-hop
Command Mode： Admin mode
Usage Guide： Display the state information of anycast rp, and display the mrt node information generated in the non first hop RP which is currently maintained by the protocol, that is the mrt node information which is created after the first hop RP transfers the register message it received to this RP.
Example：
Switch(config)#show ip pim anycast-rp non-first-hop

IP Multicast Routing Table

(*,G) Entries: 0
(S,G) Entries: 1
(E,G) Entries: 0

INCLUDE (2002:1:111::2, ff1e::2)

Local .l..... Display	Explanation
Entries	The number of all kinds of entries
INCLUDE	The mrt information created in the first hop RP.

2.3.3.9 show ipv6 pim anycast-rp status

Command：show ipv6 pim anycast-rp status

Command Mode： Admin mode.

Usage Guide： Display the configuration information of ANYCAST RP, whether ANYCAST RP globally enables, whether the self-rp-address is configured and the list of currently configured anycast rp set.

Example：

Switch(config)#show ipv6 pim anycast-rp status

Anycast RP status:
anycast-rp:Enabled!

self-rp-address:2004::2

anycast-rp address: 2000:1:111::2
other rp unicast rp address: 2002::1
other rp unicast rp address: 2005::1

anycast-rp address: 2003::1
other rp unicast rp address: 2002::2

Display	Explanation
anycast-rp:	Whether the anycast rp switch is globally enabled
self-rp-address:	The configured self-rp-address
anycast-rp address:	The configured anycast-rp-address
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address
anycast-rp address:	The configured anycast-rp-address*
other rp unicast rp address:	The configured other RP communication addresses in accordance with the above anycast-rp-address

2.3.4 ANYCAST RPv6 Configuration Examples

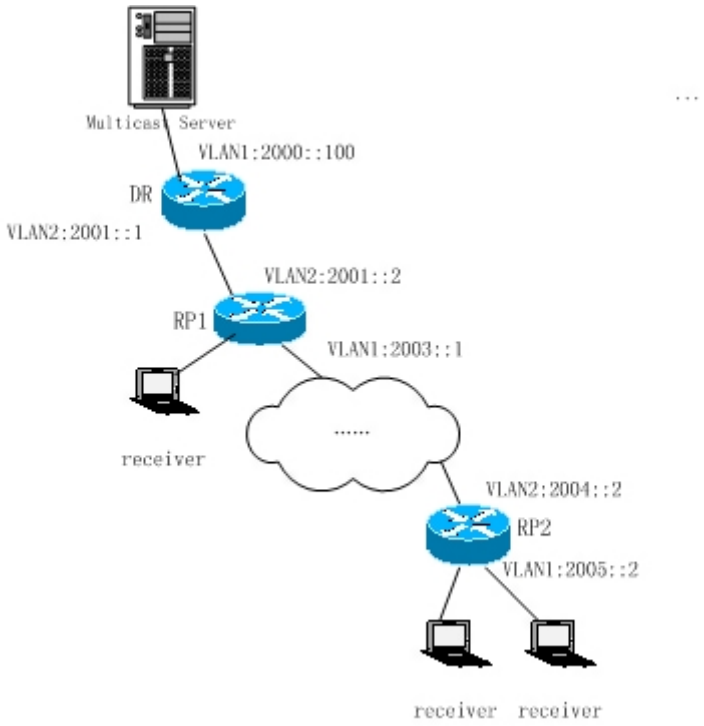


Fig 2-3 The ANYCAST RPv6 function of a router

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

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

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

2.3.5 ANYCAST RPv6 Troubleshooting Help

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 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 pim anycast-rp” or “debug ipv6 pim anycast-rp”, then copy the DEBUG information within 3 minutes and send it to the technology service center.

2.4 IPv6 DCSCM

2.4.1 IPv6 DCSCM Introduction

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

The Secure 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 Secure Controllable Multicast 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 MDL module, at the third layer, can only control the IP address sending the message.

The service-priority-oriented policy multicast of IPv6 Secure Controllable Multicast 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.

2.4.2 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 configurations 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, the 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 3 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 IGMP-SNOOPING is enabled, these rules can be globally used, or, only rules of source IP can be used in IGMP 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 mode	
ipv6 multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority> **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.

2.4.3 IPv6 DCSCM Commands

2.4.3.1 ipv6 access-list(ipv6 multicast source control)

Command: 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}

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}

Function：Configure ipv6 source control multicast access list, the no operation of this command is used to delete the access list.

Parameters：<8000-8099>：source control access list number.

{deny|permit}：deny or permit

<source/M>：the multicast source address and the length of mask.

<source-host-ip>：the multicast host address.

<destination/M>：the multicast destination address and the length of mask.

<destination-host-ip>：the multicast destination host addresses.

Default：None.

Command Mode：Global configuration mode.

Usage Guide：IPV6 multicast source control entries control the ACL it uses with ACL number 8000-8099. This command is used to configure such ACLs. IPV6 multicast source control ACL only needs to configure the source IPV6 address and destination IPV6 address (that is the group IPV6 addresses)which are to be controlled. The configuration adopts a method similar to other ACLs, which can either be an address range configured by the length of mask, or a specified host address or all addresses. Pay attention to that: for group IPV6 addresses, the “all addresses” mentioned here is ff:/8.

Example：

Switch(config)#ipv6 access-list 8000 permit fe80::203:228a/64 ff1e::1/64

Switch(config)#

2.4.3.2 ipv6 access-list(multicast destination control)

Command: ipv6 access-list <9000-10999> {deny|permit} {{<source/M> }|{host-source <source-host-ip>}|any-source} {{<destination/M> }|{host-destination <destination-host-ip>}|any-destination}

no ipv6 access-list <9000-10999> {deny|permit} {{<source/M> }|{host-source <source-host-ip>}|any-source} {{<destination/M> }|{host-destination <destination-host-ip>}|any-destination}

Function： Configure IPV6 destination control multicast access list. The no operation of this command is used to delete the access list.

Parameters： <9000-10999>：the source control access list number

{deny|permit}：deny or permit

<source/M>：the multicast source address and the length of mask

<source-host-ip>：multicast source host address

<destination/M>：multicast destination address and the length of mask

<destination-host-ip>：multicast destination host address

Default：None.

Command Mode：Global configuration mode.

Usage Guide： IPv6 multicast destination control entries control the ACL it uses with ACL number 9000-10999. This command is used to configure such ACLs. IPV6 multicast source control ACL only needs to configure the source IPv6 address and destination IPV6 address (that is the group IPV6 addresses) The configuration adopts a method similar to other ACLs, which can either be a address range configured by the length of mask, or a specified host address or all addresses Which are to be controlled. Pay attention to that: for group IPV6 addresses, the “all addresses” mentioned here is ff:/8.

Example：

Switch(config)#ipv6 access-list 9000 permit fe80::203:228a/64 ff1e::1/64

Switch(config)#

2.4.3.3 ipv6 multicast destination-control access-group

Command: ipv6 multicast destination-control access-group <9000-10999>

no ipv6 multicast destination-control access-group <9000-10999>

Function：Configure the IPV6 multicast destination control access list used by the port, the no operation of the command will delete this configuration.

Parameters：<9000-10999>：destination control access list number.

Default: Not configured.

Command Mode：Port configuration mode.

Usage Guide：This command can only take effect when the IPV6 multicast destination control is globally enabled. After configuring this command, if the MLD-SNOOPING is enabled, when adding the port to the multicast group, it will be matched according to the configured access list. Only when the port is matched as permit, will it be added, or, it can not be added.

Example：

Switch(config)#interface ethernet 1/4

Switch(Config-If-Ethernet1/4)#ipv6 multicast destination-control access-group 9000

Switch(Config-If-Ethernet1/4)#

2.4.3.4 ipv6 multicast destination-control access-group (sip)

Command: ipv6 multicast destination-control <IPADDRESS/M> access-group <9000-10999>

no ipv6 multicast destination-control <IPADDRESS/M> access-group <9000-10999>

Function：Configure the IPV6 multicast destination access list used by the specified IPv6 address, the no operation of this command will delete this configuration.

Parameters：<IPADDRESS/M>:IPv6 address and mask ; <9000-10999>：destination access list number.

Default：Not configured.

Command Mode：Global mode.

Usage Guide：This command can only take effect when the IPV6 multicast destination control is globally enabled. After configuring this command, if the MLD-SNOOPING or MLD is enabled, when adding the port to the multicast group, it will be matched according to the configured access list. Only when the port is matched as permit, will it be added, or, it can not be added. This command uses the format of “<IPADDRESS> <IPADDRESS>” on layer-two switches to match, while use the format of <IPADDRESS/M> on layer-three switches.

Example：

Switch(config)#ipv6 multicast destination-control 2008::8/64 access-group 9000

Switch(config)#

2.4.3.5 ipv6 multicast destination-control access-group (vmac)

Command: ipv6 multicast destination-control <1-4094> <macaddr> access-group <9000-10999>

no ipv6 multicast destination-control <1-4094> <macaddr> access-group <9000-10999>

Function：Configure the IPV6 multicast destination access list used by the specified vlan-mac, the no operation of this command will delete this configuration.

Parameters：<1-4094>：VLAN-ID; <macaddr>：the source MAC address sending MLD-REPORT, the format of which is ”xx-xx-xx-xx-xx-xx”; <9000-10999>：destination access list number.

Default：Not configured.

Command Mode：Global mode.

Usage Guide：This command can only take effect when the IPV6 multicast destination control is globally enabled. After configuring this command, if the MLD-SNOOPING is enabled, when adding the port to the multicast group, it will be matched according to the configured access list. Only when the port is matched as permit, will it be added, or, it can not be added.

Example：

Switch(config)#ipv6 multicast destination-control 1 00-01-03-05-07-09 access-group 9000

2.4.3.6 ipv6 multicast policy

Command: ipv6 multicast policy <IPADDRSRC/M> <IPADDRGRP/M> cos <priority>

no ipv6 multicast policy <IPADDRSRC/M> <IPADDRGRP/M> cos

Function：Configure IPV6 policy multicast, the no operation of this command is to cancel the policy multicast of IPV6.

Parameters：<IPADDRSRC/M>：the source address and the length of the mask of IPV6 multicast.

<IPADDRGRP/M>：the multicast address of IPV6 and the length of mask of multicast address

<priority>：the specified priority, the range of which is <0-7>

Default：Not configured.

Command Mode：Global configuration mode.

Usage Guide：Using this command to configure can change the priority of the multicast data which is confined by the act of matching of this switch to a specified value, and, set the TOS to the same value simultaneously. This command uses the format of “<IPADDRSRC/M>

<IPADDRGRP/M>” on layer-two switches to match, while use the format of <IPADDRESS/M> on layer-three switches. Please pay attention to that, for the messages sent in UNTAG mode, their priority will not be changed.

Example：

Switch(config)#ipv6 multicast policy 2008::1/64 ff1e::3/64 cos 4

Switch(config)#

2.4.3.7 ipv6 multicast source-control

Command: ipv6 multicast source-control

no ipv6 multicast source-control

Function： Configure to globally enable IPV6 multicast source control, the no operation of this command is to recover and globally disable the IPV6 multicast source control

Parameters： None.

Default：Disabled.

Command Mode：Global configuration mode

Usage Guide： Only when the IPV6 multicast source control is globally enabled, the source control access list can be applied to ports. After configuring this command, the IPV6 multicast data received by all the ports will be dropped by the switch if there is no matched multicast source control entry, that it only the multicast data matched as PERMIT can be received and forwarded.

Example：

Switch(config)#ipv6 multicast source-control

Switch(config)#

2.4.3.8 ipv6 multicast source-control access-group

Command: ipv6 multicast source-control access-group <8000-8099>

no ipv6 multicast source-control access-group <8000-8099>

Function：Configure the multicast source control access list used by ports, the no operation of this command is used to delete the configuration.

Parameters：<8000-8099>：source control access list number.

Default： Not Configured.

Command Mode：Port configuration mode.

Usage Guide：This command can only be successfully configured when the IPV6 multicast source control is globally enabled. After configuring this command, all the IPV6 multicast messages entering from the port will be matched according to the configured access list. Only when the message is matched as permit, can it be received and forwarded, or it will be dropped.

Example：

Switch(config)#interface ethernet 1/4

Switch(Config-If-Etherne1/4)#ipv6 multicast source-control access-group 8000

2.4.3.9 multicast destination-control

Command: multicast destination-control
no multicast destination-control

Function：Configure to globally enable IPV4 and IPV6 multicast destination control. After configuring this command, IPV4 and IPV6 multicast destination control will take effect at the same time. The no operation of this command is to recover and disable the IPV4 and IPV6 multicast destination control globally.

Parameters：None.

Default：Disabled.

Command Mode：Global configuration mode.

Usage Guide：Only after globally enabling the multicast destination control, the other destination control configuration can take effect. The destination access list can be applied to ports, VLAN-MAC and SIP. After configuring this command, IGMP-SNOOPING, MLD-SNOOPING and IGMP, MLD will match according to the rules mentioned above when they try to add ports after receiving IGMP-REPORT and MLD-REPORT.

Example：

Switch(config)# multicast destination-control
Switch(config)#

2.4.3.10 show ipv6 multicast destination-control

Command: show ipv6 multicast destination-control [detail]
show ipv6 multicast destination-control interface <Interfacename> [detail]
show ipv6 multicast destination-control host-address <ipv6addr> [detail]
show ipv6 multicast destination-control <vlan-id> <mac> [detail]

Function：Display IPV6 multicast destination control configuration.

Parameters：detail: whether to display detailed information.

<Interfacename>：interface name, such as Ethernet1/1,port-channel 1 or ethernet 1/1.

<ipv6addr>：IPV6 address

<vlan-id> ：Vlan id

<mac>：MAC address

Default：None.

Command Mode：Admin mode.

Usage Guide：Use this command to display the configured multicast destination control rules, if including the detail option, it will also display the details of the access-list in use.

Example：

Switch(config)#show ipv6 multicast destination-control

ipv6 multicast destination-control is enabled

ipv6 multicast destination-control 2003::1/64 access-group 9003

ipv6 multicast destination-control 1 00-03-05-07-09-11 access-group 9001

multicast destination-control access-group 6000 used on interface Ethernet1/13

Switch(config)#

2.4.3.11 show ipv6 multicast destination-control access-list

Command: show ip multicast destination-control access-list

show ip multicast destination-control access-list <9000-10999>

Function：Display the configured IPV6 destination control multicast access list.

Parameters：<9000-10099>: Access list number.

Default：None.

Command Mode：Admin mode.

Usage Guide：Use this command to display the configured destination control multicast access list.

Example：

Switch#show ipv6 multicast destination-control access-list

ipv6 access-list 9000 permit 2003::2/64 ff1e::3/64

ipv6 access-list 9000 deny 2008::1/64 ff1e::1/64

ipv6 access-list 9000 permit any-source any-destination

ipv6 access-list 9001 deny any-source host-destination ff1a::1

ipv6 access-list 9001 permit any-source any-destination

2.4.3.12 show ipv6 multicast policy

Command: show ipv6 multicast policy

Function：Display the configured IPV6 multicast policy.

Parameters：None.

Default：None.

Command Mode：Admin mode.

Usage Guide：Use this command to display the configured IPV6 multicast policy.

Example：

Switch#show ipv6 multicast policy

ipv6 multicast-policy 2003::2/64 ff1e::3/64 cos 5

2.4.3.13 show ipv6 multicast source-control

Command: show ipv6 multicast source-control [detail]

show ipv6 multicast source-control interface <Interfacename> [detail]

Function：Display IPV6 multicast source control configuration.

Parameters：detail: whether to display detailed information.

<Interfacename>：interface name, such as Ethernet1/1,port-channel 1 or ethernet 1/1.

Default：None.

Command Mode：Admin mode.

Usage Guide：Use this command to display the configured multicast source control rules, if including the detail option, it will also display the details of the access-list in use.

Example：

Switch#show ipv6 multicast source-control detail

Ipv6 multicast source-control is enabled

Interface Ethernet 1/1 use multicast source control access-list 8000

ipv6 access-list 8000 permit 2003::2/64 ff1e::3/64

ipv6 access-list 8000 deny 2008::1/64 ff1e::1/64

ipv6 access-list 8000 permit any-source any-destination

2.4.3.14 show ipv6 multicast source-control access-list

Command: show ipv6 multicast source-control access-list

show ipv6 multicast source-control access-list <8000-8099>

Function：Display the configured IPV6 source control multicast access list.

Parameters：<8000-8099>: Access list number.

Default：None.

Command Mode：Admin mode.

Usage Guide：Use this command to display the configured source control multicast access list.

Example：

Switch#show ipv6 multicast source-control access-list

ipv6 access-list 8000 permit 2003::2/64 ff1e::3/64

ipv6 access-list 8000 deny 2008::1/64 ff1e::1/64

2.4.4 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 Ethernet1/5 can send multicast data, and the group of data should be ff1e::1. The uplink port Ethernet1/25 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 Ethernet1/5
Switch(Config-If-Ethernet1/5)#ipv6 multicast source-control access-group 8000
Switch(config)#interface Ethernet1/25
Switch(Config-If-Ethernet1/25)#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).

2.4.5 IPv6 DCSCM Troubleshooting help

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

SCM (source control multicast） is not supported by EM4700BD-12GT-RJ45, M4700BD-12GX-SFP, EM4700BD-24TX4GC.

2.5 MLD

2.5.1 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.

2.5.2 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

2.5.3 Command for MLD

2.5.3.1 ipv6 mld access-group

Command:ipv6 mld access-group {<*acl_name*>}

no ipv6 mld access-group

Function: Configure the access control of the interface to MLD groups ;the "**no ipv6 mld access-group**" command stops the access control

Parameter: <*acl-name*> is the name of IPv6 access-list

Default:no filter condition

Command Mode: Interface Configuration Mode

Usage Guide: Configure the interface to filter MLD groups,allow or deny some group's join.

Example: Configure the interface vlan2 to accept group FF1E::1:0/112 and deny others

Switch (config)# ipv6 access-list aclv6 permit FF1E::1:0/112

Switch (config)# ipv6 access-list aclv6 deny any

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 mld access-group aclv6

2.5.3.2 ipv6 mld access-group

Command: ipv6 mld access-group {<*acl_name*>}

no ipv6 mld access-group

Function: Configure the filter conditions of the interface on the MLD group; the "**no ipv6 mld access-group**" command cancels the filter conditions.

Parameter: <*acl-name*> is the name of the IPv6 access list

Default: No filter condition by default

Command Mode: Interface Mode

Usage Guide: This command can configure the filter on the interface to the groups, permitting or denying certain groups.

Example: Configure the interface vlan1 to permit group FF1E::1:0/112, while denying all others.

Switch (config)# ipv6 access-list aclv6 permit FF1E::1:0/112

Switch (config)# ipv6 access-list aclv6 deny any

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 mld access-group aclv6

2.5.3.3 ipv6 mld immediate-leave

Command: ipv6 mld immediate-leave group-list {<*acl-name*>}

no ipv6 mld immediate-leave

Function: Configure MLD to work in the immediate leave mode,that's when the host sends a membership qualification report that equals to leave a group,the router doesn't send query and consider there is no this group's member in the subnet.The **"no ipv6 mld immediate-leave**" command cancels the immediate leave mode

Parameter: <*acl-name*> is the name of IPv6 access-list

Default: Do not configure immediate-leave group

Command Mode: Interface Configuration Mode

Usage Guide: This command is used only when there is only one host in the subnet

Example: Configure access-list"aclv6"as immediate leave mode

Switch(Config-if-Vlan1)#ipv6 mld immediate-leave group-list aclv6

2.5.3.4 ipv6 mld join-group

Command: ipv6 mld join-group <*address*>

no ipv6 mld join-group <address>

Function: Configure the interface to join in certain multicast group; the "**no ipv6 mld join-group <address>**" command cancels joining certain multicast group.

Parameter: <*address*> is a valid IPv6 multicast address

Default: No multicast group joined by factory default

Command Mode: Interface Mode

Usage Guide: The address range of the IPv6 multicast is FFxy::/8, however the (FF02::/16) is permanent addresses which can not be joined in.

Example: Join the interface vlan2 in multicast group with multicast address of ff1e::1:3.

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)#ipv6 mld join-group ff1e::1:3

2.5.3.5 ipv6 mld join-group mode source

Command: ipv6 mld join-group <*X:X::X:X*> mode <*include*|*exclude*> source <*.X:X::X:X*>

no ipv6 mld join-group <X:X::X:X> source <.X:X::X:X>

Function: Configure the sources of certain multicast group which the interface join in. Note: because of the client group has got only INLCUDE and EXCLUDE modes, if the source mode is not in accordance with current mode configured, the group mode will be changed and the original sources of the other modes configured will be cleared permanently; the “no” form of this command cancels joining certain group.

Parameter: *<X:X::X:X>* is a valid IPv6 multicast address

<include|exclude>:joining mode

<.X:X::X:X>:source list, configure several sources is allowed.

Default: No multicast group to be joined by factory default

Command Mode: Interface Mode

Usage Guide: The address range of the IPv6 multicast is FFxy::/8, however the (FF02::/16) is permanent addresses which can not be joined in. As for sources with mode same as the original one, the source will be added, while for those with different modes, the original sources will be cleared.

Example:

Join vlan2 in multicast group with multicast address of ff1e::1:3, with sources 2003::1 and 2003::2 in INCLUDE mode.

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)#ipv6 mld join-group ff1e::1:3 mode include source 2003::1 2003::2

2.5.3.6 ipv6 mld last-member-query-interval

Command: ipv6 mld last-member-query-interval <*interval*>

no ipv6 mld last-member-query-interval

Function: Configure the interface’s sending interval of querying specific group. The **“no ipv6 mld last-member-query-interval**” command cancels the manually configured value and restores the default value.

Parameter: *<interval>* is the interval of querying specific group, it ranges from 1000 to 25500ms. It’s the integer times of 1000ms. If it’s not the integer times of 1000ms, the system will convert it

to the integer times of 1000ms

Default: Defalut: 1000ms.

Command Mode: Interface Configuration Mode

Example: Configure the interface vlan1's MLD last-member-query-interval as 2000

Router(config)#int vlan 1

Router(Config-if-vlan1)#ipv6 mld last-member-query-interval 2000

2.5.3.7 ipv6 mld limit

Command:ipv6 mld limit <*state-count*>

no ipv6 mld limit

Function: Configure the MLD state count limit of the interface; the "**no ipv6 mld limit**" command restores the manually configured value to default value

Parameter:<*state-count*>:max MLD state the interface maintains, the valid range is 1-5000.

Default: 400 by default

Command Mode: Interface Mode

Usage Guide: When max state-count is configured, the number of the state the interface saves will only upper to the state-count limit; and when the max state-count is reached, the later new member qualification report received will be ignored. If some MLD group state has already been saved before this command configured, the original states will be removed and the MLD general query will be sent to collect group member qualification reports no more than the max state-count.

Example: Set the MLD state-count limit of the interface vlan2 to 4000

Switch(config)#interface vlan2

Switch(Config-if-Vlan2)#ipv6 mld limit 4000

2.5.3.8 ipv6 mld query-interval

Command: ipv6 mld query-interval <*time_val*>

no ipv6 mld query-interval

Function: Configure the interval of the periodically sent MLD host-query messages; the "**no ipv6 mld query-interval**" command restores the default value.

Parameter: <*time_val*> is the interval of the periodically sent MLD host-query messages; it ranges from 0 to 65535s

Default: Intrerval of periodically transmitted MLD query message is 125s.

Command Mode: Interface Configuration Mode

Usage Guide: When a interface enables a kind of multicast protocol,it will send MLD host-query messages periodically.This command is used to configure the query period

Example: Configure the interval of the periodically sent MLD host-query messages to 10s

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 mld query-interval 10

2.5.3.9 ipv6 mld query-max-response-time

Command: ipv6 mld query-max-response-time <*time_val*>

no ipv6 mld query- max-response-time

Function: Configure the maximum of the response time of MLD queries; the "**no ipv6 mld query- max-response-time**: command restores the default value

Parameter: <*time_val*> is the maximum of the response time of MLD queries, it ranges from 1 to 25s.

Default: 10s.

Command Mode: Interface Configuration Mode

Usage Guide: When the switch receives a query message,the host woll set a timer to each multicast group.The timer's value is between 0 to the maximum response time. When any one of the timers decreases to 0, the host will group member announce messages.Configuring the maximum response time reasonablely,the host can swiftly response to the query messages and the router can also get the group members' existing states quickly.

Example: Configure the maximum response time of MLD queries to 20s

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 mld query- max-response-time 20

2.5.3.10 ipv6 mld query-timeout

Command: ipv6 mld query-timeout <*time_val*>

no ipv6 mld query-timeout

Function: Configure the interface's timeout of MLD queries; the "**no ipv6 mld query-timeout**" command restores the default value

Parameter: <*time_val*> is the timeout of MLD queries, it ranges from 60 to 300s

Default: Default: 255s

Command Mode: Interface Configuration Mode

Usage Guide: In the share network,when there are more switches that run MLD,one switch will be selected as the querying host and others set a timer to inspect the querying host's state. If no querying packet is received when the timeout is over, a switch wiil be reselected as the querying host .

Example: Configure the interface's timeout of MLD queries to 100s

Switch (config)#interface vlan 1

Switch(Config-if-Vlan1)#ipv6 mld query-timeout 100

2.5.3.11 ipv6 mld static-group

**Command: ipv6 mld static-group <*group_address*> [*source <source_address>]*
no ipv6 mld static-group <group_address> [source <source_address>]**

Function: Configure certain static group or static source on the interface. The “no” form of this command cancels certain previously configured static group or static source

Parameter:<group_address> is a valid IPv6 multicast address;<source_address> is a valid IPv6 unicast address.

Default: No static group or static source is configured on the interface by factory default.

Command Mode: Interface Mode

Usage Guide: The valid range of the static group multicast address configured by the interface is the dynamic multicast address specified by the IPv6 protocol. Once the interface configures static group or static source for the multicast address, no matter whether there is membership qualification report of this group or source in the subnet, MLD protocol will consider that the group or source exist. Note: the configured static source is the source to be forwarded.

Example: Configure an MLD static-group ff1e::1:3 on interface vlan2

Switch(config)#interface vlan 2

Switch(Config-if-Vlan2)#ipv6 mld static-group ff1e::1:3

Configure a static source 2001::1 of the group ff1e::1:3 on interface vlan2

Switch(config)#int vlan2

Switch(Config-if-Vlan2)#ipv6 mld static-group ff1e::1:3 source 2001::1

2.5.3.12 ipv6 mld version

**Command: ipv6 mld version <*version_no*>
no ipv6 mld version**

Function: Configure the version of the MLD protocol running on the interface; the “**no ipv6 mld version**” command restores the manually configured version to the default one

Parameter: <*version_no*> is the version number of the MLD protocol,with a valid range of 1-2.

Default: 2 by default

Command Mode: Interface Mode

Usage Guide: While there is routers still not upgraded to version 2 of MLD protocol on the subnet connected, the interface should be configured to corresponding version.

Example: Configure the MLD version to 2.

Switch(config)#ipv6 mld version 2

2.5.4 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.

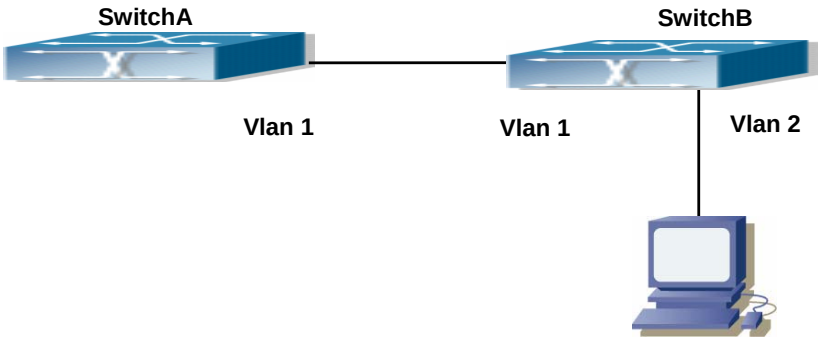


Fig 2-4 Network Topology Diagram

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

2.5.5 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.

2.5.5.1 Monitor And Debug Command

2.5.5.1.1 debug ipv6 mld events

Command: debug ipv6 mld events

debug ipv6 mld events

Function: Enable the debug switch that diaplays MLD events.the **"no debug ipv6 mld events**" command disables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: This switch can be enabled to get MLD events information

Example:

Switch# debug ipv6 mld events

Switch#1970/01/01 07:30:13 IMI: MLD Report recv: src fe80::203:fff:fe12:3457 for ff1e::1:3

1970/01/01 07:30:13 IMI: Processing Report comes from Vlan1, ifindex 2003

1970/01/01 07:30:13 IMI: MLD(Querier) ff1e::1:3 (Vlan1): No Listeners --> Listeners Present

2.5.5.1.2 debug ipv6 mld packet

Command: debug ipv6 mld packet

no debug ipv6 mld packet

Function: Enable the debug switch that diaplays MLD packets.The **"no debug ipv6 mld events**" command disables the debug switch.

Parameter: None

Default: Disabled

Command Mode: Admin Mode

Usage Guide: This switch can be enabled to get MLD packets information.

Example:

Switch# deb ipv6 mld packet

Switch#1970/01/01 07:33:12 IMI: Recv MLD packet

1970/01/01 07:33:12 IMI: Type: Listener Report (131)

1970/01/01 07:33:12 IMI: Code: 0

1970/01/01 07:33:12 IMI: Checksum: 3b7a

1970/01/01 07:33:12 IMI: Max Resp Delay: 0

1970/01/01 07:33:12 IMI: Reserved: 0

1970/01/01 07:33:12 IMI: Multicast Address: ff1e::1:3

1970/01/01 07:33:12 IMI: MLD Report recv: src fe80::203:fff:fe12:3457 for ff1e::1:3

1970/01/01 07:33:12 IMI: Processing Report comes from Vlan1, ifindex 2003

1970/01/01 07:33:12 IMI: MLD(Querier) ff1e::1:3 (Vlan1): Listeners Present --> Listeners Present

2.5.5.1.3 show ipv6 mld groups

Command: show ipv6 mld groups [{*<ifname* | *group_addr>*}]

Function: Display the MLD group information

Parameter: ***<ifname>*** is the name of the interface . Display the MLD group information. ***<group_addr>*** is the group address.Display the specified group information.

Default: Do not display

Command Mode: Admin Mode

Example:

Switch#sh ipv6 mld group

MLD Connected Group Membership

Group Address	Interface	Uptime	Expires
ff1e::1:3	Vlan1	00:00:16	00:03:14

Switch#

Displayed Information	Explanations
Group Address	Multicast group IP address
Interface	The interface of multicast group
Uptime	The existing time of the multicast group
Expires	The left time to overtime

2.5.5.1.4 show ipv6 mld interface

Command: show ipv6 mld interface [<***ifname***>]

Function: Display the relavent MLD information of an interface

Parameter: ***<ifname>*** is the name of the interface . Display the MLD information of a specific interface.

Default: Do not display

Command Mode: Admin Mode

Example: Display the MLD information of the Ethernet Interface vlan1

Switch#show ipv6 mld interface Vlan1

Interface Vlan1(2003)

Index 2003

Internet address is fe80::203:fff:fe01:e4a
MLD querier
MLD query interval is 100 seconds
MLD querier timeout is 205 seconds
MLD max query response time is 10 seconds
Last member query response interval is 1000 ms
Group membership interval is 210 seconds
MLD is enabled on interface

2.6 MLD Snooping

2.6.1 MLD Snooping Introduction

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.

2.6.2 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*> 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 specify vlan. The "no" form of this command cancels the immediate leave configuration.

ipv6 mld snooping vlan <*vlan-id*> query-mrsp <*value*> **no ipv6 mld snooping vlan <*vlan-id*> query-mrsp**	Configure the query maximum response period. The "no" form of this command 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

2.6.3 Commands For MLD Snooping Configuration

2.6.3.1 debug mld snooping all/packet/event/timer/mfc

Command: debug mld snooping all/packet/event/timer/mfc

no debug mld snooping all/packet/event/timer/mfc

Function: Enable the debugging of the switch MLD Snooping; the "no" form of this command disables the debugging.

Command Mode: Admin Mode

Default: The MLD Snooping Debugging of the switch is disabled by default

Usage Guide: This command is used for enabling the switch MLD Snooping debugging, which displays the MLD data packet message processed by the switch——packet, event messages——event,timer messages——timer,messages of down streamed hardware entry——mfc,all debug messages——all.

2.6.3.2 ipv6 mld snooping

Command: ipv6 mld snooping

no ipv6 mld snooping

Function: Enable the MLD Snooping function on the switch; the "**no ipv6 mld snooping**" command disables MLD Snooping

Command Mode: Global Mode

Default:MLD Snooping disabled on the switch by default

Usage Guide: Enable global MLD Snooping on the switch, namely allow every vlan to be configured with MLD Snooping; the "no" form of this command will disable MLD Snooping on all the vlans as well as the global MLD snooping

Example: Enable MLD Snooping under global mode.

Switch (config)#ipv6 mld snooping

2.6.3.3 ipv6 mld snooping vlan

Command: ipv6 mld snooping vlan <*vlan-id*>

no ipv6 mld snooping vlan <*vlan-id*>

Function: Enable MLD Snooping on specified vlan; the “no” form of this command disables MLD Snooping on specified vlan.

Parameter: <*vlan-id*> is the id number of the vlan,with a valid range of <1-4094>.

Command Mode: Global Mode

Default: MLD Snooping disabled on vlan by default

Usage Guide: To configure MLD snooping on certain vlan, the global MLD snooping should be first enabled. Disable MLD snooping on specified vlan with the no ipv6 mld snooping vlan vid” command

Example: Enable MLD snooping on vlan 100 under global mode.

Switch (config)#ipv6 mld snooping vlan 100

2.6.3.4 ipv6 mld snooping vlan immediate-leave

Command: ipv6 mld snooping vlan <*vlan-id*> immediate-leave

no ipv6 mld snooping vlan <*vlan-id*> immediate-leave

Function: Enable immediate-leave function of the MLD protocol in specified vlan; the “no” form of this command disables the immediate-leave function of the MLD protocol

Parameter: <*vlan-id*> is the id number of specified VLAN,with valid range of <1-4094>.

Command Mode: Global Mode

Default: Disabled by default

Usage Guide: Enable the immediate-leave function of the MLD protocol will hasten the process the port leaves one multicast group, in which the specified group query of the group will not be sent and the port will be directly deleted.

Example: Enable the MLD immediate-leave function on vlan 100

Switch (config)#ipv6 mld snooping vlan 100 immediate-leave

2.6.3.5 ipv6 mld snooping vlan l2-general-querier

Command: ipv6 mld snooping vlan < *vlan-id* > l2-general-querier

no ipv6 mld snooping vlan < *vlan-id* > l2-general-querier

Function: Set the vlan to Level 2 general querier

Parameter: *vlan-id*: is the id number of the VLAN, with a valid range of <1-4094>

Command Mode: Global Mode

Default: vlan is not a MLD Snooping L2 general querier by default.

Usage Guide: It is recommended to configure an L2 general querier on a segment. If before configure with this command, MLD snooping is not enabled on this vlan, this command will no be executed. When disabling the L2 general querier function, MLD snooping will not be disabled along with it. Main function of this command is sending general queries periodically to help the switches within this segment learn mrouter port.

Comment: There are three ways to learn mrouter port in mld snooping:

1. The port which receives MLD query messages
2. The port which receives multicast protocol packets and support PIM
3. The port statically configured.

Example: Set vlan 100 to L2 general querier.

Switch (config)# ipv6 mld snooping vlan 100 l2-general-querier

2.6.3.6 ipv6 mld snooping vlan limit

Command: ipv6 mld snooping vlan < *vlan-id* > limit {group <*g_limit*> | source <*s_limit*>}

no ipv6 mld snooping vlan < *vlan-id* > limit

Function: Configure number of groups the MLD snooping can join and the maximum number of sources in each group.

Parameter: *vlan-id*: vlan id, the valid range is <1-4094>

g_limit:<1-65535>,max number of groups joined

s_limit:<1-65535>,max number of source entries in each group, consisting of include source and exclude source

Command Mode: Global Mode

Default: Maximum 50 groups by default, with each group capable with 40 source entries.

Usage Guide: When number of joined group reaches the limit, new group requesting for joining in will be rejected for preventing hostile attacks. To use this command, MLD snooping must be enabled on vlan. The “no” form of this command restores the default other than set to “no limit”. For the safety considerations, this command will not be configured to “no limit”. It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example: Switch(config)#ipv6 mld snooping vlan 2 limit group 300

2.6.3.7 ipv6 mld snooping vlan mrouter-port interface

Command: ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface [<*ethernet*>|<*port-channel*>]<*ifname*>

no ipv6 mld snooping vlan <*vlan-id*> mrouter-port interface [<*ethernet*>|<*port-channel*>]<*ifname*>

Function: Set the static mrouter port of the vlan; the “no” form of this command cancels the

configuration.

Parameter: *vlan-id*: vlan id, the valid range is<1-4094>

ehternet:name of Ethernet port

ifname:Name of interface

***port-channel*: port aggregate**

Command Mode: Global Mode

Default: When a port is made static and dynamic mrouter port at the same time, it's the static mrouter properties is preferred. Deleting the static mrouter port can only be done with the "no" form of this command.

Example: Switch(config)#ipv6 mld snooping vlan 2 mrouter-port interface ethernet

2.6.3.8 ipv6 mld snooping vlan mrpt

Command: ipv6 mld snooping vlan <*vlan-id*> mrpt <*value*>

no ipv6 mld snooping vlan <*vlan-id*> mrpt

Function: Configure the keep-alive time of the mrouter port.

Parameter: *vlan-id*: vlan id, the valid range is <1-4094>

value:mrouter port keep-alive time with a valid range of <1-65535> secs.

Command Mode: Global Mode

Default: 255s

Usage Guide: This configuration is applicable on dynamic mrouter port, but not on static mrouter port. To use this command, MLD snooping must be enabled on the vlan.

Example: Switch(config)#ipv6 mld snooping vlan 2 mrpt 100

2.6.3.9 ipv6 mld snooping vlan query-interval

Command: ipv6 mld snooping vlan <*vlan-id*> query-interval <*value*>

no ipv6 mld snooping vlan <*vlan-id*> query-interval

Function: Configure the query interval

Parameter: *vlan-id*: vlan id, the valid range is <1-4094>

value:query interval, valid range: <1-65535>secs.

Command Mode: Global Mode

Default: 125s

Usage Guide: It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example:

Switch(config)#ipv6 mld snooping vlan 2 query-interval 130

2.6.3.10 ipv6 mld snooping vlan query-mrsp

Command: ipv6 mld snooping vlan <*vlan-id*> query-mrsp <*value*>

no ipv6 mld snooping vlan <*vlan-id*> query-mrsp

Function: Configure the maximum query response period. The “no” form of this command restores the default value.

Parameter: ***vlan-id***: vlan id, the valid range is<1-4094>

value: the valid range is <1-25> secs .

Command Mode: Global Mode

Default: 10s

Usage Guide: It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example:

Switch(config)#ipv6 mld snooping vlan 2 query-mrsp 18

2.6.3.11 ipv6 mld snooping vlan query-robustness

Command: ipv6 mld snooping vlan <vlan-id> query-robustness <*value*>

no ipv6 mld snooping vlan <vlan-id> query-robustness

Function: Configure the query robustness; the “no” form of this command restores to the default value

Parameter: ***vlan-id***: vlan id, the valid range is <1-4094>

value: the valid range is <2-10>.

Command Mode: Global Mode

Default: 2

Usage Guide: It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.

Example:

Switch(config)#ipv6 mld snooping vlan 2 query- robustness 3

2.6.3.12 ipv6 mld snooping vlan static-group

command：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>

Function： Configure static-group on specified port of the vlan. The no form of the command cancels this configuration.

Parameter: ***vlan-id***: ranging between <1-4094>

X:X::X:X:The address of group or source.

ethernet: Name of Ethernet port

port-channel: Port aggregation

ifname: Name of interface

Command Mode: Global mode

Default: No configuration by default.

Usage Guide: When a group is a static while also a dynamic group, it should be taken as a static group. Deleting static group can only be realized by the no form of the command.

Example:

Switch(config)#ip igmp snooping vlan 1 static-group ff1e::15 source 2000::1 interface ethernet 1/1

2.6.3.13 ipv6 mld snooping vlan suppression-query-time

Command: ipv6 mld snooping vlan <*vlan-id*> suppression-query-time <*value*>

no ipv6 mld snooping vlan <*vlan-id*> suppression-query-time

Function: Configure the suppression query time; the “no” form of this command restores the default value.

Parameter: ***vlan-id***: vlan id, valid range: <1-4094>

value: valid range: <1-65535>secs.

Command Mode: Global Mode

Default: 255s

Usage Guide: This command can only be configured on L2 general querier. The Suppression-query-time represents the period the suppression state maintains when general querier receives queries from layer 3 MLD within the segment. To use this command, the query-intervals in different switches within the same segment must be in accordance. It is recommended to use the default value.

Example:

Switch(config)#ipv6 mld snooping vlan 2 suppression-query-time 270

2.6.3.14 show ipv6 mld snooping

Command: show ipv6 mld snooping [vlan <*vlan-id*>]

Parameter: <*vlan-id*> is the number of vlan specified to display the MLD Snooping messages

Command Mode: Admin Mode

Usage Guide: If no vlan number is specified, it will show whether the global MLD snooping is enabled and layer 3 multicast protocol is running, as well as on which vlan the mld snooping is enabled and configured l2-general-querier. If a vlan number is specified, the detailed MLD Snooping messages of this vlan will be displayed.

Example:

Summary of the switch MLD snooping

Switch(config)#show ipv6 mld snooping

Global mld snooping status: Enabled

L3 multicasting: running

Mld snooping is turned on for vlan 1(querier)

Mld snooping is turned on for vlan 2

Displayed Information	Explanation
Global mld snooping status	Whether or not the global mld snooping is enabled on the switch
L3 multicasting	Whether or not the layer 3 multicast protocol is running on the switch.
Mld snooping is turned on for vlan 1(querier)	On which vlan of the switch is enabled mld snooping, if the vlan are l2-general-querier.

2. Display the detailed MLD Snooping information of vlan1

Switch#show ipv6 mld snooping vlan 1

Mld snooping information for vlan 1

Mld snooping L2 general querier :Yes(COULD_QUERY)

Mld snooping query-interval :125(s)

Mld snooping max reponse time :10(s)

Mld snooping robustness :2

Mld snooping mrouter port keep-alive time :255(s)

Mld snooping query-suppression time :255(s)

MLD Snooping Connect Group Membership

Note:*-All Source, (S)- Include Source, [S]-Exclude Source

Groups	Sources	Ports	Exptime	System Level
Ff1e::15	(2000::1)	Ethernet1/8	00:04:14	V2
	(2000::1)	Ethernet1/8	00:04:14	V2

Mld snooping vlan 1 mrouter port

Note:"!"-static mrouter port

!Ethernet1/2

Displayed information	Explanation
Mld snooping L2 general querier	whether or not l2-general-querier is enabled on vlan, the querier display status is set to could-query or suppressed
Mld snooping query-interval	Query interval time of the vlan
Mld snooping max reponse time	Max response time of this vlan
Mld snooping robustness	Robustness configured on the vlan
Mld snooping mrouter port	Keep-alive time of the dynamic mrouter on this vlan

keep-alive time	
Mld snooping query-suppression time	timeout of the vlan as l2-general-querier at suppressed status.
MLD Snooping Connect Group Membership	Group membership of the vlan, namely the correspondence between the port and （S,G）.
Mld snooping vlan 1 mrouter port	Mrouter port of the vlan, including both static and dynamic.

2.6.3.15 show mac-address-table multicast

Command: show mac-address-table multicast [vlan <*vlan-id*>]

Function: Display the information of multicast MAC address table

Parameter: <*vlan-id*> ,the VLAN ID included in the entries to be displayed.

Command Mode: Admin Mode

Default: Mapping between the multicast MAC address and port is not displayed by system default.

Usage Guide: This command shows the information on multicast address table of current switch.

Example: Show the multicast mapping in vlan 100

```
Switch#show mac-address-table multicast vlan 100
Vlan Mac Address                    Type      Ports
---- --------------------------- ------- ---------------------------------------
100  01-00-5e-01-01-01              MULTI Ethernet
```

2.6.4 MLD Snooping Examples

Scenario 1: MLD Snooping Function

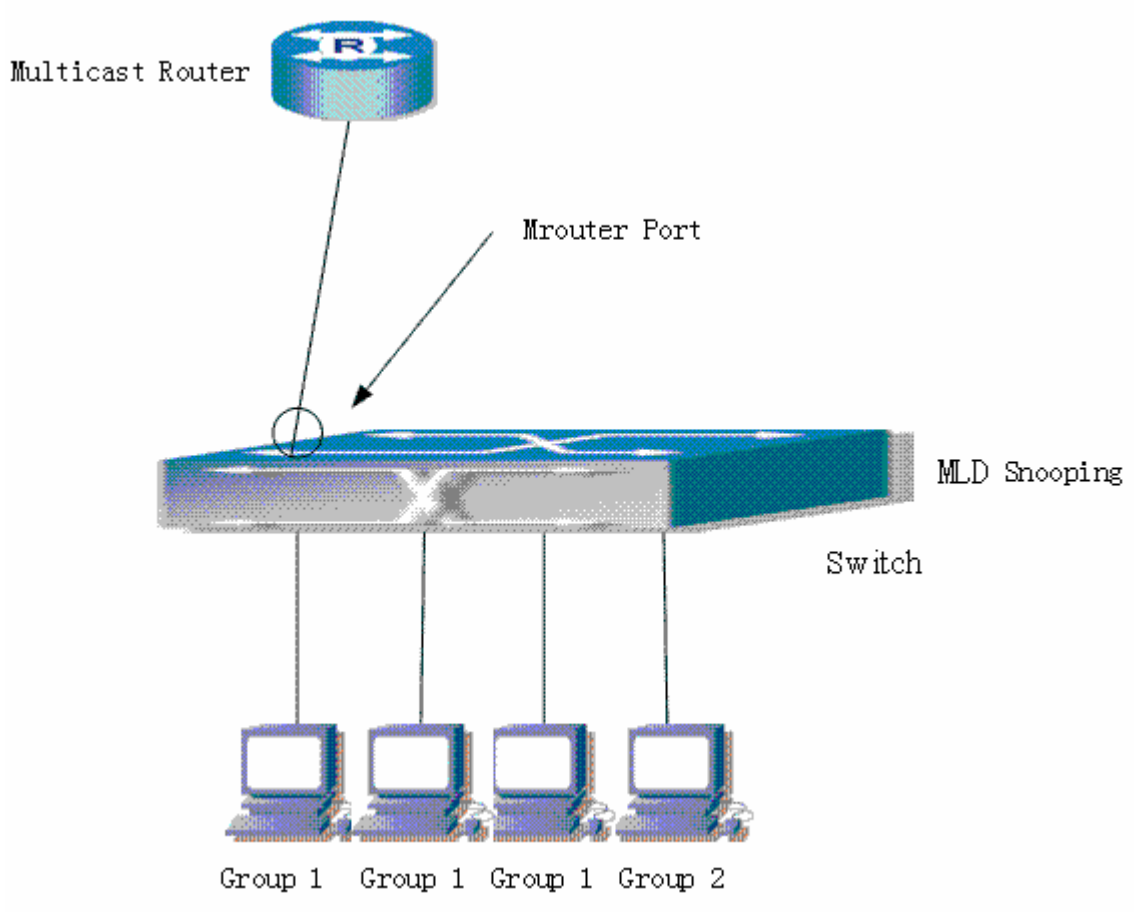


Fig 2-5 Switches as MLD Querier Function figure

As shown above, the vlan 100 configured on the switch consists of ports 1, 2, 6, 10, 12. Four hosts are respectively connected to 2, 6, 10, 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 1/1

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

and 5 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: port1, 2 and 6 are in （Multicasting Server 1, Group1）, port1, 10 are in (Multicasting Server 1,Group2), and port1, 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.

MLD L2-general-querier

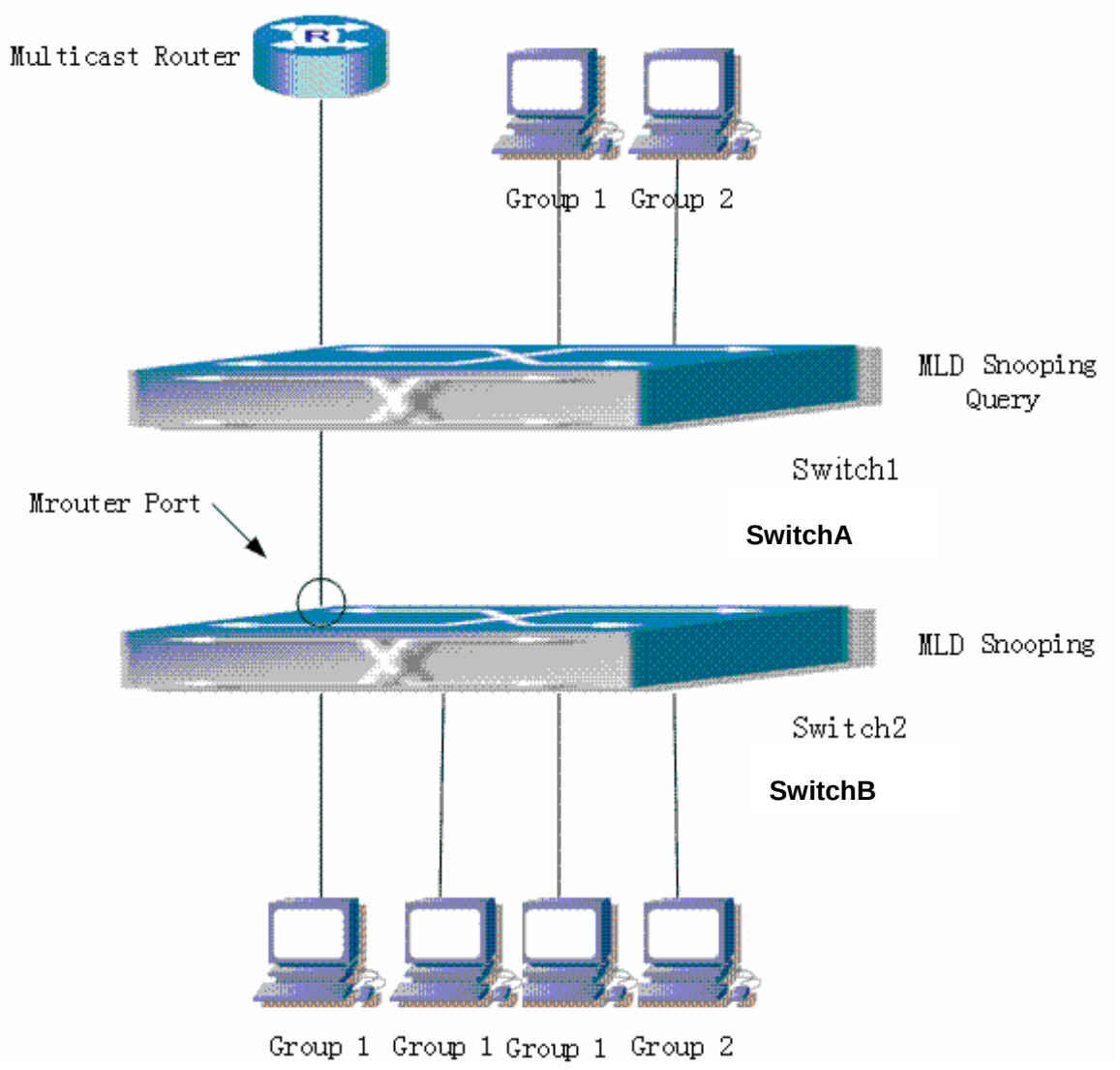


Fig 2-6 Switches as MLD Querier Function figure

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, 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 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 1/1

Multicast configuration

Same as scenario 1

MLD Snooping interception results:

Same as scenario 1

2.6.5 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:

(3) Ensure the physical connection is correct

(4) Ensure the MLD Snooping is enabled under global mode (using ipv6 mld snooping)

(5) Ensure the MLD Snooping is configured on the vlan under global mode (using ipv6 mld snooping vlan <vlan-id>）

(6) Ensure there is a vlan configured as a L2 general querier, or there is a static mrouter configured in a segment,

(7) Use command to check if the MLD snooping information is correct.

If the MLD Snooping problem remain unsolved, please use debug mld snooping and other debugging command and copy the DEBUG message within 3 minutes, send the recorded message to the technical server center of our company.

Chapter 3 Multicast VLAN

3.1 Introduction 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

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 config 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

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

Command	Explanation
Global Mode	
ipv6 mld snooping vlan <*vlan-id*> **no ipv6 mld snooping vlan <*vlan-id*>**	Enable the MLD Snooping function on the multicast vlan. The "no” form of this command disables the MLD Snooping on the 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 Commands For Multicast VLAN

3.3.1 multicast-vlan

Command:multicast-vlan

no multicast-vlan

Function: Enable multicast VLAN function on a VLAN; the “no” form of this command disables the multicast VLAN function.

Parameter: None

Command Mode: VLAN config Mode

Default: Multicast VLAN function not enabled by default

Usage Guide: The multicast VLAN function can not be enabled on private VLAN. To disabling the multicast VLAN function of the VLAN, configuration of VLANs associated with the multicast VLAN should be deleted. Note that the default vlan can not be configured with this command and only one multicast vlan is allowed on a switch

Examples:

Switch(config)#vlan 2

Switch (Config-Vlan2)# multicast-vlan

3.3.2 multicast-vlan association

Command:multicast-vlan association *<vlan-list>*

no multicast-vlan association *<vlan-list>*

Function: Associate several VLANs with a multicast VLAN; the “no” form of this command cancels the association relations.

Parameter: *<vlan-list>* the VLAN ID list associated with multicast VLAN. Each VLAN can only be associated with one multicast VLAN and the association will only succeed when every VLAN listed in the VLAN ID table exists.

Command Mode: VLAN mode

Default: The multicast VLAN is not associated with any VLAN by default

Usage Guide: After a VLAN is associated with the multicast VLAN, when there comes the multicast order in the port of this VLAN, then the multicast data will be sent from the multicast VLAN to this port, so to reduce the data traffic. The VLAN associated with the multicast VLAN should not be a Private VLAN. A VLAN can only be associated with another VLAN after the multicast VLAN is enabled. Only one multicast VLAN can be enabled on a switch.

Examples:

Switch(config)#vlan 2

Switch (Config-Vlan2)#multicast-vlan

Switch (Config-Vlan2)# multicast-vlan association 3;4

3.4 Examples Of Multicast VLAN

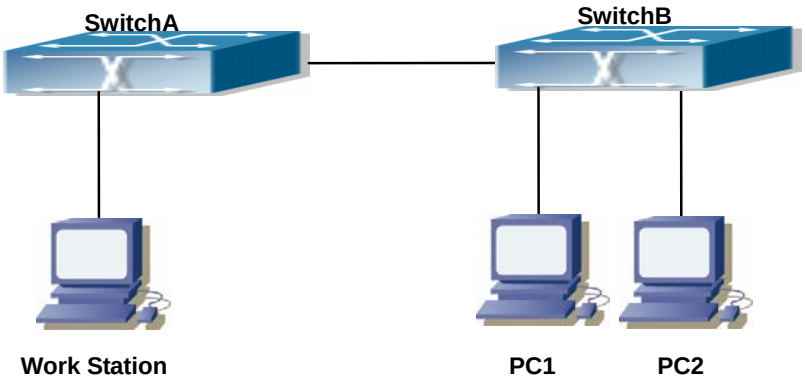


Fig 3-1 Function configuration of the Multicast VLAN

As shown in the figure, the multicast server is connected to the layer 3 switch switchA through port 1/1 which belongs to the vlan10 of the switch. The layer 3 switch switchA is connected with layer 2 switches through the port 1/10,which configured as trunk port. On the

switchB the vlan100 is configured set to contain port 1/15, and vlan101 to contain port 1/20. PC1 and PC2 are respectively connected to port 1/15 and 1/20. The switchB is connected with the switchA through port 1/10, 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 interface ethernet 1/1
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 ethernet1/10
SwitchA(Config-If-Ethernet1/10)switchport mode trunk

SwitchB#config
SwitchB(config)#vlan 100
SwitchB(config-vlan100)#Switchport interface ethernet 1/15
SwitchB(config-vlan100)exit

SwitchB(config)#vlan 101
SwitchB(config-vlan101)#Switchport interface ethernet 1/20
SwitchB(config-vlan101)exit

SwitchB(config)# interface ethernet 1/10
SwitchB(Config-If-Ethernet1/10)#Switchport mode trunk
SwitchB(Config-If-Ethernet1/10)#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
```

The principle is same to use IPv4 multicast when multicast VLAN supports IPv6 multicast. But the IPv6 multicast cooperates with MLD snooping. There are no more examples.