Content

Chapter 1 IPv4 Multicast Protocol

1.1 Public Commands for Multicast

1.1.1 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

1.2 Commands for PIM-DM

1.2.1 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 nsm, debug pim mfc, debug pim timer, debug pim state, refer to PIM-SM handbook.

1.2.2 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.
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.

1.2.3 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 will 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> <.ifname>, the first one is ingress interface, follow is egress interface.
Default: To delete this static multicast entry, if the command isn't included interface parameter.
Command Mode: Global Mode.
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. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified interface will be removed.
Example:
Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30

1.2.4 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 receive 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

1.2.5 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

1.2.6 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)#

1.2.7 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)#

1.2.8 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)#

1.2.9 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

1.2.10 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

1.2.11 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)#

1.2.12 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

1.2.13 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

1.2.14 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

1.2.15 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        ..l.....................

(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     ..o....................

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

1.2.16 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.

1.2.17 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	Type	Nexthop Num	Nexthop Addr	Nexthop Ifindex	Nexthop Name	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 Commands for PIM-SM

1.3.1 clear ip pim bsr rp-set

Command: clear ip pim bsr rp-set *
Function: Clear all RP.
Parameters: None.
Command Mode: Admin Configuration Mode
Usage Guide: Clear all RP rapidly.
Example: Clear all RP.
Switch# clear ip pim bsr rp-set *
Relative Command: show ip pim bsr-router

1.3.2 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
Switch#

1.3.3 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

1.3.4 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.
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 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

1.3.6 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

1.3.7 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

1.3.8 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

1.3.9 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
Switch#

1.3.10 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 will 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*> <*.ifname*>, the first one is ingress interface, follow is egress interface.
Default: To delete this static multicast entry, if the command isn't included interface parameter.
Command Mode: Global Mode.
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. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified interface will be removed.
Example:
Switch(config)#ip mroute 10.1.1.1 225.1.1.1 v10 v20 v30

1.3.11 ip multicast unresolved-cache aging-time

Command: ip multicast unresolved-cache aging-time <value>
no ip multicast unresolved-cache aging-time
Function: Configure the cache time of the kernel multicast route, the no command restores the default value.
Parameter: < value> is the configured cache time, ranging between 1 and 20s.
Default: 20s.
Command Mode: Global Configuration Mode.
Usage Guide: Configure the cache time of multicast route entry in kernel.
Example:
Switch(config)# ip multicast unresolved-cache aging-time 18

1.3.12 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***>: **<*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
Switch (config)#

1.3.13 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 receive 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

1.3.14 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 with other candidate BSRs for the BSR router. 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 with other candidate BSRs for the BSR router. 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

1.3.15 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 register packet'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 used to interact with older Cisco IOS version.
Example: Configure the register packet's checksum of the group specified by myfilter to use the whole packet's length.
Switch (config)#ip pim cisco-register-checksum group-list 23

1.3.16 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)#

1.3.17 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)#

1.3.18 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 neighbor holdtime,if the switch hasn't received the neighbor hello packets when the holdtime is over, this neighbor 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 Hold time'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 denied. 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)#

1.3.19 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 oriented each other and determine neighbor relationship. Pim switch announce the existence of itself by periodically transmitting hello messages to neighbors. If no hello messages from neighbors are received in the certain time, the neighbor is considered lost. This value can't be greater than neighbor 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)#

1.3.20 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 configures 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

1.3.21 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 timer
Switch (config)#ip pim jp-timer 59

1.3.22 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
Switch (config)#

1.3.23 ip pim neighbor-filter

Command: ip pim neighbor-filter <*list-number*>
no ip pim neighbor-filter <*list-number*>
Function: Configure the neighbor 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 connection 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" is not configured, deny 10.1.4.10 0.0.0.255 is the same as deny any.
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
Switch (config)#show ip pim neighbor

1.3.24 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 59p/s.

Switch (config)#ip pim register-rate-limit 59
Switch (config)#

1.3.25 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
Switch (config)#

1.3.26 ip pim register-source

Command: ip pim register-source {<*A.B.C.D*> | <*ifname*>| 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 usually the RPF neighbor of source host direction.

Parameter: <*ifname*> is the interface name,
<*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

1.3.27 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
Switch (config)#

1.3.28 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 doesn'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)#

1.3.29 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* isVlan 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

1.3.30 ip pim rp-register-kat

Command: ip pim rp-register-kat <*vaule*>
no ip pim rp-register-kat
Function: This command is to configure 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 keep alive time, during the keep alive 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 keep alive time is over, this item will be obsolete.
Example: Configure the kat value of RP's (S, G) item to 180s
Switch (config)#ip pim rp-register- kat 180
Switch (config)#

1.3.31 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

1.3.32 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)#

1.3.33 show ip pim bsr-router

Command: show ip pim bsr-router
Function: Display BSR address
Parameter: None
Default: None
Command Mode: Admin 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

1.3.34 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

1.3.35 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       ..I.....................
  Joined      .....................
  Asserted    .....................
  Outgoing    ..o.....................
```

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 interface, 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.

1.3.36 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.

1.3.37 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      Type  Nexthop  Nexthop        Nexthop   Nexthop
Metric Pref  Refcnt
                       Num      Addr           Ifindex   Name
____
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

1.3.38 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: Group 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

1.3.39 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 Commands for MSDP Configuration

1.4.1 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: *seconds*: the units are seconds, 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

1.4.2 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 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

1.4.4 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 Peers.
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 *

1.4.5 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 sources 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 items 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. 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

1.4.6 clear msdp statistics

Command: clear msdp statistics {*peer-address*| *}
Function: To clear MSDP statistic information, and not reset the session of MSDP Peer.
Parameter: *peer-address*: The IP address of Peer.
***** Disconnection with all the Peers.
Command Mode: Admin Mode.
Usage Guide: None.
Example:
Switch#clear msdp statistics *

1.4.7 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.

Usage Guide: The router use the IP address of this port to set up MSDP Peer connection with MSDP Peer. Pay attention: specified connect-source address must consitant with the configuration of Peer address, otherwise can not set up TCP connection. The configuration under MSDP Peer mode will cover with MSDP Mode. No command will cancel the configuration and set again all the MSDP connection of this port.
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

1.4.8 debug msdp all

Command: debug msdp all
no debug msdp all
Function: To enable all the debugging information about MSDP; the no command disable all the debugging information.
Command Mode: Admin Configuration Mode.
Default: Disabled.
Usage Guide: Enable the debugging switch of MSDP, display the protocol packet send/receive information of MSDP Peer---packet, keepalive packet send/receive information---keepalive, event information---event, NSM mutual information---nsm, timer information---timer, protocol state information---fsm, filter policy information---filter.
Exampe:
Switch#debug msdp all

1.4.9 debug msdp events

Command: debug msdp events
no debug msdp events
Function: Enable /disable the 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

1.4.10 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

1.4.11 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

1.4.12 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 enables this switch.
Example:
Switch#debug msdp keepalive

1.4.13 debug msdp nsm

Command: debug msdp nsm
no debug msdp nsm
Function: Enable/disable the switch of **msdp nsm debug**.
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

1.4.14 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

1.4.15 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

1.4.16 debug msdp timer

Command: debug msdp timer
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

1.4.17 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

1.4.18 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-20

1.4.19 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

1.4.20 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

1.4.21 originating-rp

Command: originating-rp <*interface-type*> <*interface-number*>
no originating-rp
Function: Configure Originating RP address that 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*>: type and number of the port.
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

1.4.22 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 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. Pay attention: specified Peer address must be corresponded with the interface address. If configure the Connect-source, the Peer address must be Connect-source interface address; if not specified Connect-source, the Peer address is the egress address, otherwise cannot set up TCP connection.

Example: To configure MSDP Peer in MSDP congfiguration mode.
Switch(config-msdp)#peer 10.1.1.1
Switch(config-msdp-peer)#

1.4.23 redistribute

Command: redistribute [list <*acl-list-number* | *acl-name*>]
no redistribute
Function: To configure the redistribute of SA messages.
Parameter: ***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

1.4.24 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 from 1 to 65535.
Command Mode: MSDP Peer Configuration Mode.
Default: The AS number isn't initialized to 0 by default.
Usage Guide: This command set the AS number for specified Peer. The no command restores the AS number of specified MSDP Peer.
Example:
Switch(config)#router msdp
Switch(router-msdp)#peer 20.1.1.1
Switch(router-msdp-peer)# remote-as 20

1.4.25 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

1.4.26 sa-filter

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 controls 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, the entire SA messages 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
```

1.4.27 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
```

1.4.28 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 messages from MSDP Peer will be filtered.
Parameter: *access-list-number*: The ACL number, it 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 messages 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

1.4.29 show msdp global

Command: show msdp global
Function: Show the configuration information in MSDP Mode.
Command Mode: Admin and Configuration Mode.
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:
   test-1
```

The introduction of showed items:

Field	Explaination
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.

1.4.30 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

1.4.31 show msdp peer

Command: show msdp peer {A.B.C.D}
Function: Show the configuration information in MSDP Mode.
Parameter: A.B.C.D: MSDP Peer Address.
Command Mode: Admin and Configuration Mode.
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 Rrjected:     0
      SA messages outgoing Rrjected:     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	Explaination
MSDP Peer	IP address of MSDP Peer.
AS	Autonomous system number belonged toMSDP Peer.
State	MSDP Peer state.
Connection source	The interface used in local TCP connection.
Uptime(Downtime)	The uptime or downtime of MSDP peer.
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.
SAs learned from this peer	The SA numbers learned from MSDP Peers in the cache.
SAs limit	The configured SA limit numbers with this MSDP Peer.

1.4.32 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: Admin and Configuration Mode.
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	Explaination
(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.

1.4.33 show msdp sa-cache summary

Command: show msdp sa-cache summary
Function: Show the summary of MSDP Cache.
Command Mode: Admin and Configuration Mode.
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	Explaination
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.

1.4.34 show msdp statistics

Command: show msdp statistics peer [*Peer-address*]
Function: Show all the statistics of specified Peer or receiving/sending messages from all the Peers.
Parameter: Peer-address: Show the statistics of messages from specified Peer.
Command Mode: Admin and Configuration Mode.
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
The introduction of showed items:

Field	Explaination
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.

1.4.35 show msdp summary

Command: show msdp summary
Function: Show the summary of MSDP.
Command Mode: Admin and Configuration Mode.
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	Explaination
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.

1.4.36 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 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
```

1.4.37 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 from 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
```

1.5 Commands for ANYCAST RP v4

1.5.1 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

1.5.2 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 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 RP 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 RP 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 RP communicating with this router (as a RP). The unicast address identifies other RP, 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 RP in the network to notify all the RP in the network of the source (S.G) state. While forwarding, the router will change the destination address of the register message into other-rp-address.
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 RP 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

1.5.4 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 RP, and to communicate with other RP. The no operation of this command will cancel the configured unicast address used by this router (as a RP) to communicate with other RP.
Parameters: *self-rp-addr*: The unicast address used by this router (as a RP) to communicate with other RP.
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 RP in the network, notifying them of the state of source (S.G). While forwarding the register message, this router will change the source address of it into self-rp-address.
2. Once this router(as a RP) receives a register message from other RP unicast, such as a register message whose destination is the self-rp-address of this router, it will create (S,G) state and send back a register-stop message, whose destination address is the source address of the register message.
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

1.5.5 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

1.5.6 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

1.5.7 show ip pim anycast-rp first-hop

Command: show ip pim anycast-rp first-hop
Command Mode: Admin and Configuration 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.

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

Command: show ip pim anycast-rp non-first-hop
Command Mode: Admin and Configuration 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.

1.5.9 show ip pim anycast-rp status

Command: show ip pim anycast-rp status
Command Mode: Admin and Configuration 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.

1.6 Commands for PIM-SSM

1.6.1 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 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)#ip multicast ssm range 23

1.7 Commands for DVMRP

1.7.1 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.

1.7.2 ip dvmrp enable

Command: ip dvmrp enable
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 executing DVMRP protocol on interface.
Example: Enable DVMRP Protocol on interface vlan1.
Switch (config)#interface vlan 1
Switch(Config-If-vlan1)#ip dvmrp enable

1.7.3 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 metric value, value range from 1 to 31
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 judgment, 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

1.7.4 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: Default
Command Mode: Global Mode
Usage Guide: Dvmrp multicast-protocol can enable after globally execute the command
Example: Switch (config)#ip dvmrp multicast-routing

1.7.5 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

1.7.6 ip dvmrp reject-non-pruners

Command: ip dvmrp reject-non-pruners
no ip dvmrp reject-non-pruners
Function: Configure to reject neighbor ship with DVMRP router of non pruning/grafting on the interface, the "**no ip dvmrp reject-non-pruners**" command restores neighbor ship 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

1.7.7 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: 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 packets packed in unicast data packets, 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

1.7.8 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

1.7.9 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

1.7.10 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 neighbor

Neighbor Address	Interface	Uptime/Expires	Maj Ver	Min Ver	Cap 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

1.7.11 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 Address	Mask Len	Group Address	State	FCR Exptime	Prune/Graft 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

1.7.12 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

1.8 Commands for DCSCM

1.8.1 access-list (Multicast Destination Control)

Command: access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}
no access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any} {{<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-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 only 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 character to 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
Switch(config)#

1.8.2 access-list (Multicast Source Control)

Command: access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip>}|any-destination}
no access-list <5000-5099> {deny|permit} ip {{<source> <source-wildcard>}|{host <source-host-ip>}|any} {{<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-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 Multicast source 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 only 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 character to 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

1.8.3 ip multicast destination-control

This command is not supported by the switch.

1.8.4 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)#inter e 1/0/4
Switch(Config-If-Ethernet 1/0/4)#ip multicast destination-control access-group 6000
Switch (Config-If-Ethernet1/0/4)#

1.8.5 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 established before executing the command, it needs to execute 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

1.8.6 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

1.8.7 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 packet, 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

1.8.8 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

1.8.9 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)#interface ethernet1/0/4
Switch (Config-If-Ethernet1/0/4)#ip multicast source-control access-group 5000
Switch (Config-If-Ethernet1/0/4)#
Switch(router-msdp)#default-rpf-peer 10.0.0.1 rp-policy 10

1.8.10 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 and IGMP will match according to the rules mentioned above when they try to add ports after receiving IGMP-REPORT.
Example:
switch(config)# multicast destination-control

1.8.11 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 Ethernet1/0/1, port-channel 1 or ethernet1/0/1.
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 Ethernet1/0/13

switch(config)#

1.8.12 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 any-destination
access-list 6000 deny ip any host-destination 224.1.1.1
access-list 6000 deny ip host 2.1.1.1 any-destination
access-list 6001 deny ip host 2.1.1.1 225.0.0.0 0.255.255.255
access-list 6002 permit ip host 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

1.8.13 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

1.8.14 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 1/0/1 or ethernet1/0/1.
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 enabled
Interface Ethernet1/0/13 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

1.8.15 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

1.9 Commands for IGMP

1.9.1 clear ip igmp group

Command: clear ip igmp group [A.B.C.D | IFNAME]
Function: Delete the group record of the specific group or interface.
Parameters: A.B.C.D the specific group address; IFNAME the specific interface.
Command Mode: Admin Configuration Mode
Usage Guide: Use show command to check the deleted group record.
Example: Delete all groups.
Switch#clear ip igmp group
Relative Command: show ip igmp group

1.9.2 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

1.9.3 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

1.9.4 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

1.9.5 ip igmp immediate-leave

Command: ip igmp immediate-leave group-list {<number>|<name>}
no ip igmp immediate-leave
Function: Configure 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)#

1.9.6 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 diffence 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

1.9.7 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 transmitting 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 automatically 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

1.9.8 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: 0, no limit.
Command Mode: Interface Configuration Mode
Usage Guide: After configuring maximum 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

1.9.9 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

1.9.10 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: 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: configure 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

1.9.11 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: 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

1.9.12 ip igmp robust-variable

Command: ip igmp robust-variable <value>
no ip igmp robust-variable
Function: Configure the robust variable value，the "**no ip igmp robust-variable**" command restores default value.
Parameter: value: range from 2 to 7.
Command Mode: Interface Configuration Mode
Default: 2.
Usage Guide: It is recommended using the default value.
Example:
Switch (config-if-vlan1)#ip igmp robust-variable 3

1.9.13 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 packet 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

1.9.14 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: 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

1.9.15 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

1.9.16 show ip igmp interface

Command: show ip igmp interface {vlan <*vlan_id*>|<*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
```

1.10 Commands for IGMP Snooping

1.10.1 clear ip igmp snooping vlan

Command: clear ip igmp snooping vlan <1-4094> groups [A.B.C.D]
Function: Delete the group record of the specific VLAN.
Parameters: <1-4094> the specific VLAN ID; A.B.C.D the specific group address.
Command Mode: Admin Configuration Mode
Usage Guide: Use show command to check the deleted group record.

Example: Delete all groups.
Switch#clear ip igmp snooping vlan 1 groups
Relative Command: show ip igmp snooping vlan <1-4094>

1.10.2 clear ip igmp snooping vlan <1-4094> mrouter-port

Command: clear ip igmp snooping vlan <1-4094> mrouter-port [ethernet IFNAME | IFNAME]
Function: Delete the mrouter port of the specific VLAN.
Parameters: <1-4094> the specific VLAN ID; ethernet the Ethernet port name; IFNAME the port name.
Command Mode: Admin Configuration Mode
Usage Guide: Use show command to check the deleted mrouter port of the specific VLAN.
Example: Delete mrouter port in vlan 1.
Switch# clear ip igmp snooping vlan 1 mrouter-port
Relative Command: show ip igmp snooping mrouter-port

1.10.3 debug igmp snooping all/packet/event/timer/mfc

Command: debug igmp snooping all/packet/event/timer/mfc
no debug igmp snooping all/packet/event/timer/mfc
Function: Enable the IGMP Snooping switch of the switch; the "**no debug igmp snooping all/packet/event/timer/mfc**" disables the debugging switch.
Command Mode: Admin Mode
Default: IGMP Snooping debugging switch is disabled on the switch by default.
Usage Guide: The command is used for enable the IGMP Snooping debugging switch of the switch, switch IGMP data packet message can be shown with "packet" parameter, event message with "event", timer message with "time", downsending hardware entries message with "mfc", and all debugging messages with "all".

1.10.4 ip igmp snooping

Command: ip igmp snooping
no ip igmp snooping
Function: Enable the IGMP Snooping function; the "**no ip igmp snooping**" command disables this function.
Command mode: Global Mode
Default: IGMP Snooping is disabled by default.
Usage Guide: Use this command to enable IGMP Snooping, that is permission every VLAN config the function of IGMP snooping. The "**no ip igmp snooping**" command disables this function.
Example: Enable IGMP Snooping.
Switch(config)#ip igmp snooping

1.10.5 ip igmp snooping proxy

Command: ip igmp snooping proxy
no ip igmp snooping proxy
Function: Enable IGMP Snooping proxy function, the no command disables the function.
Parameter: None.
Command Mode: Global Mode
Default: Enable.
Example:
Switch(config)#no ip igmp snooping proxy

1.10.6 ip igmp snooping vlan

Command: ip igmp snooping vlan <*vlan-id*>
no ip igmp snooping vlan <*vlan-id*>
Function: Enable the IGMP Snooping function for the specified VLAN; the "**no ip igmp snooping vlan <vlan-id>**" command disables the IGMP Snooping function for the specified VLAN.
Parameter: <*vlan-id*> is the VLAN number.
Command mode: Global Mode
Default: IGMP Snooping is disabled by default.
Usage Guide: To configure IGMP Snooping on specified VLAN, the global IGMP Snooping should be first enabled. Disable IGMP Snooping on specified VLAN with the "**no ip igmp snooping vlan <vlan-id>**" command.
Example: Enable IGMP Snooping for VLAN 100 in Global Mode.
Switch(config)#ip igmp snooping vlan 100

1.10.7 ip igmp snooping vlan immediate-leave

Command: ip igmp snooping vlan <*vlan-id*> immediate-leave
no ip igmp snooping vlan <*vlan-id*> immediate-leave
Function: Enable the IGMP Snooping fast leave function for the specified VLAN; the "**no ip igmp snooping vlan <*vlan-id*> immediate-leave**" command disables the IGMP Snooping fast leave function.
Parameter: <*vlan-id*> is the VLAN number specified.
Command mode: Global Mode
Default: This function is disabled by default.
Usage Guide: Enable immediate-leave function of the IGMP Snooping in specified VLAN; the"no" form of this command disables the immediate-leave function of the IGMP Snooping.
Example: Enable the IGMP Snooping fast leave function for VLAN 100.
Switch(config)#ip igmp snooping vlan 100 immediate-leave

1.10.8 ip igmp snooping vlan l2-general-querier

Command: ip igmp snooping vlan < *vlan-id* > l2-general-querier
no ip igmp snooping vlan < *vlan-id* > l2-general-querier
Function: Set this VLAN to layer 2 general querier.
Parameter: *vlan-id*: is ID number of the VLAN, ranging is <1-4094>.
Command Mode: Global mode
Default: VLAN is not as the IGMP Snooping layer 2 general querier.
Usage Guide: It is recommended to configure a layer 2 general querier on a segment. IGMP Snooping function will be enabled by this command if not enabled on this VLAN before configuring this command, IGMP Snooping function will not be disabled when disabling the layer 2 general querier function. This command is mainly for sending general queries regularly to help switches within this segment learn mrouter ports.
Comment: There are three paths IGMP snooping learn mrouter
1 Port receives the IGMP query messages
2 Port receives multicast protocol packets, and supports DVMRP, PIM
3 Static configured port

1.10.9 ip igmp snooping vlan l2-general-querier-source

Command: ip igmp snooping vlan <vlanid> L2-general-query-source <A.B.C.D>
no ip igmp snooping vlan <vlanid> L2-general-query-source
Function: Configure source address of query of igmp snooping
Parameters: <vlanid>: the id of the VLAN, with limitation to <1-4094>.
<A.B.C.D> is the source address of the query operation.

Command Mode: Global mode.
Default: 0.0.0.0
Usage Guide: It is not supported on Windows 2000/XP to query with the source address as 0.0.0.0. So the layer 2 query source address configuration does not function. The client will stop sending requesting datagrams after one is sent. And after a while, it can not receive multicast datagrams.
Example:
Switch(config)#ip igmp snooping vlan 2 L2-general-query-source 192.168.1.2

1.10.10 ip igmp snooping vlan l2-general-querier-version

Command: ip igmp snooping vlan <vlanid> L2-general-query-version <version>
Function: Configure igmp snooping.
Parameters: vlan-id is the id of the VLAN, limited to <1-4094>. **version** is the version number, limited to <1-3>.
Command Mode: Global mode.
Default: version 3.
Usage Guide: When the switch is connected to V1 and V2 capable environment, and for VLAN which has source of layer 2 query configuration, the VLAN can be queried only if the version number has been specified. This command is used to query the layer 2 version number.
Example:
Switch(config)#ip igmp snooping vlan 2 L2-general-query-version 2

1.10.11 ip igmp snooping vlan limit

Command: ip igmp snooping vlan <*vlan-id*> limit {group <*g_limit*> | source <*s_limit*>}
no ip igmp snooping vlan <*vlan-id*> limit
Function: Configure the max group count of VLAN and the max source count of every group. The "**no ip igmp snooping vlan <*vlan-id*> limit**" command cancels this configuration.
Parameter: <*vlan-id*> is the VLAN number.
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, IGMP 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 IGMP is in operation, please make this configuration in accordance with the IGMP configuration as possible.
Example: Switch(config)#ip igmp snooping vlan 2 limit group 300

1.10.12 ip igmp snooping vlan mrouter-port

interface

Command: ip igmp snooping vlan <*vlan-id*> mrouter-port interface[<ehternet> | <port-channel>] <ifname>
no ip igmp snooping vlan <*vlan-id*> mrouter-port interface[<ehternet> | <port-channel>] <ifname>
Function: Configure static mrouter port of VLAN. The no form of the command cancels this configuration.
Parameter: ***vlan-id***: ranging between <1-4094>
ehternet: Name of Ethernet port
ifname: Name of interface
port-channel**:** Port aggregation
Command Mode: Global mode
Default: No static mrouter port on VLAN by default.
Usage Guide: When a port is a static mrouter port while also a dynamic mrouter port, it should be taken as a static mrouter port. Deleting static mrouter port can only be realized by the no command.
Example: Switch(config)#ip igmp snooping vlan 2 mrouter-port interface ethernet1/0/13

1.10.13 ip igmp snooping vlan mrouter-port learnpim

Command: ip igmp snooping vlan <*vlan-id*> mrouter-port learnpim
no ip igmp snooping vlan <*vlan-id*> mrouter-port learnpim
Function: Enable the function that the specified VLAN learns mrouter-port (according to pim packets), the no command will disable the function.
Parameter: <*vlan-id*>: The specified VLAN ID, ranging from 1 to 4094.
Command Mode: Global Mode
Default: Enable
Usage Guide: Enable the function that the specified VLAN learns mrouter-port (according to pim packets). After a port received pim packets, it will be set to mrouter port for implementing the automatic learning.
Example: Disable the function that vlan 100 learns mrouter-port (according to pim packets).
Switch(config)#no ip igmp snooping vlan 100 mrouter-port learnpim

1.10.14 ip igmp snooping vlan mrpt

Command: ip igmp snooping vlan <*vlan-id*> mrpt <*value*>
no ip igmp snooping vlan <*vlan-id*> mrpt
Function: Configure this survive time of mrouter port.
Parameter: ***vlan-id*****:** VLAN ID, ranging between <1-4094>
value**:** mrouter port survive period, ranging between <1-65535>seconds
Command Mode: Global mode
Default: 255s
Usage Guide: This command validates on dynamic mrouter ports but not on mrouter port. To use this command, IGMP Snooping of this VLAN should be enabled previously.
Example: Switch(config)#ip igmp snooping vlan 2 mrpt 100

1.10.15 ip igmp snooping vlan query-interval

Command: ip igmp snooping vlan <*vlan-id*> query-interval <*value*>
no ip igmp snooping vlan <*vlan-id*> query-interval
Function: Configure this query interval.
Parameter: ***vlan-id***: VLAN ID, ranging between <1-4094>
value: query interval, ranging between <1-65535>seconds
Command Mode: Global mode
Default: 125s
Usage Guide: It is recommended to use the default settings. Please keep

this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.
Example: Switch(config)#ip igmp snooping vlan 2 query-interval 130

1.10.16 ip igmp snooping vlan query-mrsp

Command: ip igmp snooping vlan <*vlan-id*> query-mrsp <*value*>
no ip igmp snooping vlan <*vlan-id*> query-mrsp
Function: Configure the maximum query response period. The "**no ip igmp snooping vlan <*vlan-id*> query-mrsp**" command restores to the default value.
Parameter: ***vlan-id***: VLAN ID, ranging between <1-4094>
value: ranging between <1-25> seconds
Command Mode: Global mode
Default: 10s
Usage Guide: It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.
Example:
Switch(config)#ip igmp snooping vlan 2 query-mrsp 18

1.10.17 ip igmp snooping vlan query-robustness

Command: ip igmp snooping vlan <vlan-id> query-robustness <*value*>
no ip igmp snooping vlan <vlan-id> query-robustness
Function: Configure the query robustness. The "**no ip igmp snooping vlan <vlan-id> query-robustness**" command restores to the default value.
Parameter: ***vlan-id***: VLAN ID, ranging between <1-4094>
value: ranging between <2-10>
Command Mode: Global mode
Default: 2
Usage Guide: It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.
Example:
Switch(config)#ip igmp snooping vlan 2 query- robustness 3

1.10.18 ip igmp snooping vlan report source-address

Command: ip igmp snooping vlan <*vlan-id*> report source-address <*A.B.C.D*>
no ip igmp snooping vlan <*vlan-id*> report source-address
Function: Configure forward report source-address for IGMP, the "**no ip igmp snooping vlan <*vlan-id*> report source-address**" command restores the default setting.
Parameter: ***vlan-id*****:** VLAN ID range<1-4094>;
A.B.C.D**:** IP address, can be 0.0.0.0.
Command Mode: Global Mode.
Default: Disabled.
Usage Guide: Default configuration is recommended here. If IGMP snooping needs to be configured, the source address for forwarded IGMP messages can be 0.0.0.0. If it is required by the upstream that IGMP messages should use the same network address, the source address of IGMP messages should be configured to be the same with upstream.

Example:
Switch (config)#ip igmp snooping vlan 2 report source-address 10.1.1.1

1.10.19 ip igmp snooping vlan specific-query-mrsp

Command: ip igmp snooping vlan <vlan-id> specific-query-mrsp <value>
no ip igmp snooping vlan <vlan-id> specific-query-mrspt
Function: Configure the maximum query response time of the specific group or source, the no command restores the default value.
Parameters: <vlan-id>: the specific VLAN ID, the range from 1 to 4094. <value>: the maximum query response time, unit is second, the range from 1 to 25, default value is 1.
Command Mode: Global mode
Default: Enable the function.
Usage Guide: After enable vlan snooping in global mode, input this command to configure the maximum query response time of the specific group.
Example: Configure/cancel the specific-query-mrsp of vlan3 as 2s.
Swith(config)#ip igmp snooping vlan 3 specific-query-mrsp 2
Swith(config)#no ip igmp snooping vlan 3 specific-query-mrspt

1.10.20 ip igmp snooping vlan static-group

Command: ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet | port-channel] <IFNAME>
no ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>]interface [ethernet | port-channel] <IFNAME>
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>
A.B.C.D: 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 224.1.1.1 source 192.168.1.1 interface ethernet 1/0/1

1.10.21 ip igmp snooping vlan suppression-query-time

Command: ip igmp snooping vlan <*vlan-id*> suppression-query-time <*value*>
no ip igmp snooping vlan <*vlan-id*> suppression-query-time
Function: Configure the suppression query time. The "**no ip igmp snooping vlan <*vlan-id*> suppression-query-time**" command restores to the default value.
Parameter: ***vlan-id***: VLAN ID, ranging between <1-4094>
value: ranging between<1-65535> seconds
Command Mode: Global mode
Default: 255s

Usage Guide: This command can only be configured on L2 general querier. The Suppression-query-time refers to the period of suppression state in which the querier enters when receives query from the layer 3 IGMP in the segments.
Example: Switch(config)#ip igmp snooping vlan 2 suppression-query-time 270

1.10.22 show ip igmp snooping

Command: show ip igmp snooping [vlan <*vlan-id*>]
Parameter: <*vlan-id*> is the VLAN number specified for displaying IGMP Snooping messages.
Command Mode: Admin Mode
Usage Guide: If no VLAN number is specified, it will show whether global IGMP Snooping switch is on, which VLAN is configured with l2-general-querier function, and if a VLAN number is specified, detailed IGMP messages for this VLAN will be shown.
Example:
1. Show IGMP Snooping summary messages of the switch
Switch(config)#show ip igmp snooping
Global igmp snooping status: Enabled
L3 multicasting: running
Igmp snooping is turned on for vlan 1(querier)
Igmp snooping is turned on for vlan 2

Displayed Information	Explanation
Global igmp snooping status	Whether the global igmp snooping switch on the switch is on
L3 multicasting	whether the layer 3 multicast protocol of the switch is running
Igmp snooping is turned on for vlan 1(querier)	which VLANs on the switch is enabled with igmp snooping function, whether they are l2-general-querier

2. Display the IGMP Snooping summary messages of vlan1.
Switch#show ip igmp snooping vlan 1
Igmp snooping information for vlan 1

Igmp snooping L2 general
querier :Yes(COULD_QUERY)
Igmp snooping query-interval :125(s)
Igmp snooping max reponse time :10(s)
Igmp snooping robustness :2
Igmp snooping mrouter port keep-alive time :255(s)
Igmp snooping query-suppression time :255(s)

IGMP Snooping Connect Group Membership
Note:*-All Source, (S)- Include Source, [S]-Exclude Source
Groups Sources Ports Exptime
System Level
238.1.1.1 (192.168.0.1) Ethernet1/0/8 00:04:14
V2
(192.168.0.2) Ethernet1/0/8 00:04:14
V2

Igmp snooping vlan 1 mrouter port
Note:"!"-static mrouter port

!Ethernet1/0/2

Displayed Information	Explanation
Igmp snooping L2 general querier	Whether the VLAN enables l2-general-querier function and show whether the querier state is could-query or suppressed
Igmp snooping query-interval	Query interval of the VLAN
Igmp snooping max reponse time	Max response time of the VLAN
Igmp snooping robustness	IGMP Snooping robustness configured on the VLAN
Igmp snooping mrouter port keep-alive time	keep-alive time of dynamic mrouter of the VLAN
Igmp snooping query-suppression time	Suppression timeout of VLAN when as l2-general-querier
IGMP Snooping Connect Group Membership	Group membership of this VLAN, namely the correspondence between ports and (S,G)
Igmp snooping vlan 1 mrouter port	mrouter port of the VLAN, including both static and dynamic

1.11 Commands for IGMP Proxy

1.11.1 clear ip igmp proxy agggroup

Command: clear ip igmp proxy agggroup
Function: Delete all group records.
Parameters: None.
Command Mode: Admin Configuration Mode
Usage Guide: Use show command to check the deleted group record.
Example: Delete all groups.
Switch#clear ip igmp proxy agggroup
Relative Command: show ip igmp proxy upstream group

1.11.2 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, mfc, which disposed in the switch.
Example:
Switch# debug igmp proxy all

1.11.3 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

1.11.4 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

1.11.5 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

1.11.6 debug igmp proxy timer

Command: debug igmp proxy timer
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

1.11.7 ip igmp proxy

Command: ip igmp proxy
no ip igmp proxy
Function: Enable the IGMP Proxy function; the "**no ip igmp proxy**" command disables this function.
Command Mode: Global Mode.
Default: The switch disables 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

1.11.8 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

1.11.9 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 ip igmp proxy downstream**" command will disable the configuration.
Example: Enable IGMP Proxy downstream port function in interface VLAN2 under interface configuration mode.
Switch (config)#interface vlan 2
Switch(Config-if-Vlan2)#ip igmp proxy downstream

1.11.10 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.
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

1.11.11 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

1.11.12 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 to 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

1.11.13 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. **Parameter: *value*:** <2~10>. The retry time for upstream ports' sending unsolicited report is limited between 2 and 10.
Command Mode: Global Mode.
Default: Retry time 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

1.11.14 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 ip igmp proxy upstream**" 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

1.11.15 ip multicast ssm

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

1.11.16 ip pim bsr-border

Command: ip pim bsr-border
no ip pim bsr-border
Function: To configure the PIM enabled port to consider all 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

1.11.17 show debugging igmp proxy

Command: show debugging igmp proxy
Function: Display the status of debug switch of IGMP Proxy.
Command Mode: Admin Mode.
Usage Guide: The debuging switch status 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

1.11.18 show ip igmp proxy

Command: show ip igmp Proxy
Function: Display the IGMP Proxy configuration information.
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

1.11.19 show ip igmp proxy mroute

Command: show ip igmp Proxy mroute
Function: Display the status information of **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)

1.11.20 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

Chapter 2 IPv6 Multicast Protocol

2.1 Public Commands for Multicast

2.1.1 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: None.
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

2.2 Commands for PIM-DM6

Explain: Part SHOW and DEBUG commands is same to PIM-SM, please reference the PIM-SM command.

2.2.1 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.

2.2.2 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.

2.2.3 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. This no command deletes 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*> <*.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. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified egress interface will be removed.
Example:
Switch(config)#ipv6 mroute 2001::1 ff1e::1 v10 v20 v30

2.2.4 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 receive 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

2.2.5 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 switch. 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

2.2.6 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

2.2.7 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

2.2.8 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: Define 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, hello time will default current 3.5 times of Hello_interval. If setting hello time 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

2.2.9 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 neighbor ship. 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

2.2.10 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

2.2.11 ipv6 pim neighbor-filter

Command: ipv6 pim neighbor-filter <a*ccess-list-name*>
no ipv6 pim neighbor-filter <a*ccess-list-name*>
Function: Configure neighbor access-list. If filtered by list and connected the neighbor, the connection immediately was broken. 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 neighbor ship, 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 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

2.2.12 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: <*500-599*> 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 IPV6 PIM. The multicast data flow will not be forwarded to the SCOPE-BORDER.
Example:
Switch(Config-if-Vlan2)#ipv6 pim scope-border 503

2.2.13 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 Items 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

2.2.14 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

2.2.15 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        ..l.....................

(2000:10:1:12::11, ff1e::15)
RPF nbr: ::
RPF idx: Vlan12
Upstream State: FORWARDING
Origin State: ORIGINATOR
  Local        .....................
  Pruned       .....................
  Asserted     .....................
  Outgoing     ..o.....................

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

2.2.16 show ipv6 pim neighbor

Command: show ipv6 pim neighbor [detail|]
Function: Display router neighbors.
Parameter: None
Default: None
Command Mode: Admin and configuration Mode
Usage Guide: Display multicast router neighbors maintained by the PIM.
Example:

```
Switch(config)#show ipv6 pim neighbor
Neighbor                  Interface          Uptime/Expires    Ver
DR
Address
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 DR

2.2.17 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: Admin and configuration 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
```

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

2.3 Commands for PIM-SM6

2.3.1 clear ipv6 pim bsr rp-set

Command: clear ipv6 pim bsr rp-set *
Function: Clear all RP.
Parameters: None.
Command Mode: Admin Configuration Mode
Usage Guide: Clear all RP rapidly.
Example: Clear all RP.
Switch# clear ipv6 pim bsr rp-set *
Relative Command: show ipv6 pim bsr-router

2.3.2 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

2.3.3 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

2.3.4 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

2.3.5 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

2.3.6 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

2.3.7 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

2.3.8 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

2.3.9 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

2.3.10 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. This no command deletes 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> <.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. To removed the specified multicast routing entry. If all the egress interfaces are specified, or no interfaces are specified, the specified multicast routing entry will be removed. Otherwise the multicast routing entry for the specified egress interface will be removed.

Example:

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

2.3.11 ipv6 multicast unresolved-cache aging-time

Command: ipv6 multicast unresolved-cache aging-time <value>
no ipv6 multicast unresolved-cache aging-time

Function: Configure the cache time of kernel multicast route, the no command restores the default value.

Parameter: < value> is the configured cache time, ranging between 1 and 20s.

Default: 20s.

Command Mode: Global Configuration Mode.

Usage Guide: Configure the cache time of multicast route entry in kernel.

Example:

Switch(config)# ipv6 multicast unresolved-cache aging-time 18

2.3.12 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

2.3.13 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 receive 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

2.3.14 ipv6 pim bsr-candidate

Command: ipv6 pim bsr-candidate {vlan <vlan_id>|tunnel

<tunnel-id>|<ifname>} [<hash-mask-length>] [<priority>]
no ipv6 pim bsr-candidate {vlan <vlan_id>| tunnel <tunnel-id>|<ifname>} [<hash-mask-length>] [<priority>]
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 {vlan <vlan_id>| tunnel <tunnel-id>|<ifname>} [<hash-mask-length>] [<priority>]**" command disables the candidate BSR.
Parameter: <vlan_id> is VLAN ID ,the value ranges from 1 to 4094;
<tunnel_id> is tunnel ID,the value ranges from 1 to 50;
<*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

2.3.15 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 register packet's head length default: 8
Parameter: <*access-list name*> is the applying simple access-list.
Command Mode: Global Mode
Usage Guide: This command is used to interact with older Cisco IOS version.
Example: Configure the register packet's checksum 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

2.3.16 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

2.3.17 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

2.3.18 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 neighbor holdtime, if the switch hasn't received the neighbor hello packets when the holdtime is over, this neighbor 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 denied. 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

2.3.19 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 is 30s.
Command Mode: Interface Configuration Mode
Usage Guide: Hello messages make pim switches oriented each other and determine neighbor relationship. Pim switch announce the existence of itself by periodically transmitting hello messages to neighbors. If no hello messages from neighbors are received in the certain time, the neighbor is considered lost. This value can't be greater than neighbor 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

2.3.20 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

2.3.21 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 transmitting J/P messages to59s.
Example: Switch(config)#ipv6 pim jp-timer 59

2.3.22 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

2.3.23 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 neighbor 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 connection can't be created.
Parameter: <a*cess-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" is not configured, deny fe80:20e:cff:fe01:facc is the same as deny any. The command can configure on IPv6 tunnel interface, but it is successful configuration to only configure tunnel carefully.
Example: Configure VLAN's pim neighbor 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

2.3.24 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: Global Mode

Usage Guide: Configure the speedrate of DR sending register packets.

Example: Configure the speedrate of DR sending register packets to 59p/s.

Switch(config)#ipv6 pim Register-rate-limit 59

2.3.25 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

2.3.26 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 usually 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

2.3.27 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

2.3.28 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 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

2.3.29 ipv6 pim rp-candidate

Command: ipv6 pim rp-candidate{vlan<vlan-id> |loopback<index> |<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: <vlan_id> is VLAN ID;
<index> is Loopback interface index;
<*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: 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 announce messages
Switch (config)# ipv6 pim rp-candidate vlan1 100

2.3.30 ipv6 pim rp-register-kat

Command: ipv6 pim rp-register-kat <*vaule*>

no ipv6 pim rp-register-kat

Function: This command is to configure the KAT (KeepAlive Timer) value of the RP (S, G) items, the unit is second. The "**no ipv6 pim rp-register-kat**" command 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

2.3.31 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: <*500-599*> 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 IPV6 PIM. The multicast data flow will not be forwarded to the SCOPE-BORDER.
Example:
Switch(Config-if-Vlan2)#ipv6 pim scope-border 503

2.3.32 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

2.3.33 show ipv6 pim bsr-router

Command: show ipv6 pim bsr-router
Function: Display BSR address.
Parameter: None
Default: None
Command Mode: Admin Mode and Global 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

2.3.34 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

2.3.35 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 Configuration 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        ..I.............................
  Joined       .................................
```

```
  Asserted    .....................................
FCR:
  (2000:1:111::11, ff1e::15)
RPF nbr: ::
RPF idx: None
SPT bit: 1
Upstream State: JOINED
  Local       .....................................
  Joined      .....................................
  Asserted    .....................................
  Outgoing    ..o..................................
  (2000:1:111::11, ff1e::15, rpt)
RP: 2000:1:111::100
RPF nbr: ::
RPF idx: None
Upstream State: NOT PRUNED
  Pruned      .....................................
  Outgoing    ..o..................................
```

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 interface, this interface receive J/P messages
Asserted	Asserted state
Outgoing	Final outgoing of multicast data

2.3.36 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                  Interface          Uptime/Expires     Ver
DR
Address
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

2.3.37 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
```

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

2.3.38 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	The source of Bootstrap information

2.3.39 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

2.4 Commands for ANYCAST RP v6

2.4.1 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
```

2.4.2 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
```

2.4.3 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 RP 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 RP 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 RP, 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 RP in the network to notify all the RP in the network of the source (S.G) state. While forwarding, the router will change the destination address of the register message into other-rp-address.
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 RP one by one.
Example: Configure other-rp-address in global configuration mode.
Switch(config)#ipv6 pim anycast-rp 2000::1 2004::2

2.4.4 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 RP, and to communicate with other RP. The no operation of this command will cancel the configured unicast address used by this router (as a RP) to communicate with other RP.
Parameters: ***self-rp-addr*****:** The unicast address used by this router (as a RP) to communicate with other RP.
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 RP in the network, notifying them of the state of source (S.G). While forwarding the register message, this router will change the source address of it into self-rp-address.
2. Once this router(as a RP) receives a register message from other RP unicast, such as a register message whose destination is the self-rp-address of this router, it will create (S,G) state and send back a register-stop message, whose destination address is the source address of the register message.
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

2.4.5 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

2.4.6 show debugging ipv6 pim

Command: show debugging ipv6 pim
Command Mode: Admin and Configuration 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

2.4.7 show ipv6 pim anycast-rp first-hop

Command: show ipv6 pim anycast-rp first-hop
Command Mode: Admin and Configuration 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, ffle::1)
Local .l.....

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

2.4.8 show ipv6 pim anycast-rp non-first-hop

Command: show ipv6 pim anycast-rp non-first-hop
Command Mode: Admin and Configuration 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, ffle::2)
  Local        .l.....................
```

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

2.4.9 show ipv6 pim anycast-rp status

Command: show ipv6 pim anycast-rp status
Command Mode: Admin and Configuration 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.

2.5 Commands for PIM-SSM6

2.5.1 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

2.6 Commands for IPv6 DCSCM

2.6.1 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*>: 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>*:** 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 ACL. 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

2.6.2 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 ACL. 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

2.6.3 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>*: The 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)#inter ethernet 1/0/4
switch(Config-If-Ethernet1/0/4)#ipv6 multicast destination-control access-group 9000
switch(Config-If-Ethernet1/0/4)#

2.6.4 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 multicast destination-control access-list used on specified net segment, the "**no ipv6 multicast destination-control *<IPADDRESS/M>* access-group *<9000-10999>***"command deletes this configuration.
Parameter: *<IPADDRESS/M>*: IP address and mask length;
***<9000-10999>*:** Destination control access-list number.
Default: None.
Command Mode: Global Mode.
Usage Guide: The command is only working under global IPv6 multicast destination-control enabled, after configuring the command, if MLD-SPOOPING or MLD is enabled, for adding the members to multicast group. If configuring multicast destination-control on specified net segment of transmitted MLD-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 ipv6 mld groups detail** has been established before executing the command, it needs to execute **clear ipv6 mld group** command to clear relevant groups in admin mode.
Example:
Switch(config)#ipv6 multicast destination-control 2008::8/64 access-group 9000

2.6.5 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 of the 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 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)#ipv6 multicast destination-control 1 00-01-03-05-07-09 access-group 9000

2.6.6 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. 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

2.6.7 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 enabled globally, 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

2.6.8 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 the port, 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)#inter ethernet 1/0/4
switch(Config-If-Ethernet1/0/4)#ipv6 multicast source-control access-group 8000

2.6.9 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

2.6.10 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.
***<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 Ethernet1/0/13
switch(config)#

2.6.11 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 IPv6 destination control multicast access list.
Example:

switch# sh ipv6 multicast destination-control acc
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

2.6.12 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

2.6.13 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*>: Port name.
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 1/0/1 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

2.6.14 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#sh 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

2.7 Commands for MLD

2.7.1 clear ipv6 mld group

Command: clear ipv6 mld group [X:X::X:X | IFNAME]
Function: Delete the group record of the specific group or interface.

Parameters: X:X::X:X the specific group address; IFNAME the specific interface address.
Command Mode: Admin Configuration Mode
Usage Guide: Use show command to check the deleted group record.
Example: Delete all groups.
Switch#clear ipv6 mld group
Relative Command: show ipv6 mld group

2.7.2 debug ipv6 mld events

Command: debug ipv6 mld events
no debug ipv6 mld events
Function: Enable the debug switch that displays 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

2.7.3 debug ipv6 mld packet

Command: debug ipv6 mld packet
no debug ipv6 mld packet
Function: Enable the debug switch that displays 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

2.7.4 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

2.7.5 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

2.7.6 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 Configuration 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

2.7.7 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 Configuration 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

2.7.8 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: 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

2.7.9 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 Configuration 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

2.7.10 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

2.7.11 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 will 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

2.7.12 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: 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 will 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

2.7.13 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 Configuration 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

2.7.14 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 Configuration Mode
Usage Guide: While there are 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.
Swith(config)#interface vlan 1
Swith(config-if-vlan1)#ipv6 mld version 2

2.7.15 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

2.7.16 show ipv6 mld interface

Command: show ipv6 mld interface [<*ifname*>]
Function: Display the relevant 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

2.7.17 show ipv6 mld join-group

Command: show ipv6 mld join-group
show ipv6 mld join-group interface {vlan <*vlan_id*>|<*ifname*>}
Function: Display the join-group messages on the interfaces.
Parameters: <ifname> is the name of the interface, which means to display MLD information on the specified interface.
Default: Do not display
Command Mode: Admin and Configuration Mode.
Example: Display the MLD information on Ethernet interfaces in vlan2.
Switch#show ipv6 mld join-groups interface Vlan2
Mld join group information:
INTERFACE: Vlan2
HOST VERSION: 2
MULTICAST ADDRESS: ff1e:: 1:3
GROUP STATE: EXCLUDE
SOURCE ADDRESS: 2003::1 mode: EXCLUDE
SOURCE ADDRESS: 2003::2 mode: EXCLUDE
SOURCE ADDRESS: 2003::6 mode: EXCLUDE
SOURCE ADDRESS: 2003::9 mode: EXCLUDE

2.8 Commands for MLD Snooping Configuration

2.8.1 clear ipv6 mld snooping vlan

Command: clear ipv6 mld snooping vlan <1-4094> groups [X:X::X:X]
Function: Delete the group record of the specific VLAN.
Parameters: <1-4094> the specific VLAN ID; X:X::X:X the specific group address.
Command Mode: Admin Configuration Mode
Usage Guide: Use show command to check the deleted group record.
Example: Delete all groups.
Switch#clear ipv6 mld snooping vlan 1 groups
Relative Command: show ipv6 mld snooping vlan <1-4094>

2.8.2 clear ipv6 mld snooping vlan <1-4094> mrouter-port

Command: clear ipv6 mld snooping vlan <1-4094> mrouter-port [ethernet IFNAME|IFNAME]
Function: Delete the mrouter port of the specific VLAN.
Parameters: <1-4094> the specific VLAN ID; ethernet the Ethernet port name; IFNAME the port name.
Command Mode: Admin Configuration Mode
Usage Guide: Use show command to check the deleted group record.
Example: Delete the mrouter port in vlan 1.
Switch# clear ipv6 mld snooping vlan 1 mrouter-port

Relative Command: show ipv6 mld snooping mrouter-port

2.8.3 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.

2.8.4 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

2.8.5 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

2.8.6 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: Enabling 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

2.8.7 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

2.8.8 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

2.8.9 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 ethernet1/0/13

2.8.10 ipv6 mld snooping vlan mrouter-port learnpim6

Command: ipv6 mld snooping vlan <*vlan-id*> mrouter-port learnpim6
no ipv6 mld snooping vlan <*vlan-id*> mrouter-port learnpim6

Function: Enable the function that the specified VLAN learns mrouter-port (according to pimv6 packets), the no command will disable the function.

Parameter: <*vlan-id*>: The specified VLAN ID, ranging from 1 to 4094.

Command Mode: Global Mode

Default: Enable

Usage Guide: Enable the function that the specified VLAN learns mrouter-port (according to pimv6 packets). After a port received pimv6 packets, it will be set to mrouter port for implementing the automatic learning.

Example: Disable the function that vlan 100 learns mrouter-port (according to pimv6 packets).

Switch(config)#no ipv6 mld snooping vlan 100 mrouter-port learnpim6

2.8.11 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

2.8.12 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

2.8.13 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

2.8.14 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

2.8.15 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 1/0/1

2.8.16 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

2.8.17 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:
1. 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)	Ethernet1/0/8	00:04:14	V2
	(2000::2)	Ethernet1/0/8	00:04:14	V2

Mld snooping vlan 1 mrouter port
Note:"!"-static mrouter port
!Ethernet1/0/2

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	Keep-alive time of the dynamic mrouter on this VLAN
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.

Chapter 3 Commands for Multicast VLAN

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 Configuration 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

3.2 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 association 3, 4

3.3 multicast-vlan association interface

Command: multicast-vlan association interface (ethernet | port-channel|) IFNAME
no multicast-vlan association interface (ethernet | port-channel|) IFNAME

Function: Associate the specified port with the multicast VLAN, so the associated ports are able to receive the multicast flow. The no command cancels the association between the ports and the multicast VLAN.

Parameter: IFNAME: The name of the ethernet port or port-channel port

Command Mode: VLAN configuration mode

Default: None.

Usage Guide:

1. ‘associated VLAN’ and ‘associated port’ of the multicast VLAN are absolute, they do not affect each other when happening the cross.
2. The port of the aggregation member cannot be associated, but the associated port is able to be added to port-group and cancelling the association.
3. The configured port type includes port-channel port or ethernet port and the

port is only configured as ACCESS mode.
4. The port (it will be associated) cannot belong to the multicast VLAN, in the same way, the associated port cannot be divided in multicast VLAN.
5. When the associated port mode is set as non ACCESS mode, the mode cannot be changed.
Example: Suppose vlan2 is multicast VLAN.
Switch(config-vlan2)#multicast-vlan association interface ethernet 1/0/2
Switch(config-vlan2)#multicast-vlan association interface port-channel 2
Switch(config-vlan2)#no multicast-vlan association interface ethernet 1/0/2
Switch(config-vlan2)#no multicast-vlan association interface port-channel 2

3.4 switchport association multicast-vlan

This command is not supported by the switch.