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 IGMP

1.2.1 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

1.2.2 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

1.2.3 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

1.2.4 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

1.2.5 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)#

1.2.6 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

1.2.7 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

1.2.8 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

1.2.9 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

1.2.10 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

1.2.11 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

1.2.12 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.
Robustness Variable: The Robustness Variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may be increased. IGMP is robust to (Robustness Variable -1) packet losses. The Robustness Variable MUST NOT be 0, and SHOULD NOT be 1. Default: 2.
Example:
Switch (config-if-vlan1)#ip igmp robust-variable 3

1.2.13 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

1.2.14 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

1.2.15 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

1.2.16 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

1.3 Commands for IGMP Snooping

1.3.1 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>

1.3.2 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

1.3.3 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".

1.3.4 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

1.3.5 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

1.3.6 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

1.3.7 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

1.3.8 ip igmp snooping vlan <id> immediately-leave mac-based

Command: ip igmp snooping vlan <id> immediately-leave mac-based
no ip igmp snooping vlan <id> immediately-leave mac-based
Function: Configure this command to delete the existed igmp snooping table entries according to the source mac in leave packet when the switch which is enabled the igmp snooping function receives the leave packet. Only when the received the port, source mac and multicast group of the leave packet are the same as the port, host mac and multicast group of the existed igmp snooping table entry, the snooping table entry can be deleted. If this command is not configured, delete the existed igmp snooping table entry according to the port and multicast group of the leave packet.
Command mode: Global Mode
Default: This function is disabled by default.
Usage Guide: Configure the immediately-leave under the same vlan at the same time to make this command effective. In this time, deal with it according to the host mac of the port.
Example: Use the following configuration when delete the table entry according to the host mac of the port.
switch(config)#ip igmp snooping vlan 12 immediately-leave
switch(config)#ip igmp snooping vlan 12 immediately-leave mac-based

1.3.9 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

1.3.10 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

1.3.11 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

1.3.12 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

1.3.13 ip igmp snooping vlan interface (ethernet | port-channel|) IFNAME limit

Command: ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit {group <1-65535>| source <1-65535>} strategy (replace | drop)

no ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit group source strategy

Function: Configure the number of groups which are allowed joining and the maximum of the source in each group under the IGMP Snooping port. Configure the strategy when it is up to the upper limit, including "replace" and "drop".

Parameters: ***vlan-id***: VLAN ID range is <1-4094>

***ehternet*:** Ethernet port name

***ifname*:** Interface name

port-channel: ports aggregation

***<1-65535>*:** The maximum number of groups allowed joining

***<1-65535>*:** The maximum number of source table entries in each group, including include source and exclude source.

***replace*:** Replace the group and source information

drop**:** Drop the new group and source information

Command mode: Global Mode.

Default: There is no limitation as default.

Usage Guide: When the number of the groups joined under the port or the number of sources in this group exceeds the limit, it will be dealt according to the configured strategy. If it is drop, drop the new group and source information; if it is replace, find a dynamic group and source from the port to conduct deleting and replacing, and then add the new group and source information. The premise of using this command is that this VLAN is enabled IGMP Snooping function. No command configures as “no limitation”.

Example:

Switch(config)#ip igmp snooping vlan 2 interface ethernet 1/0/11 limit group 300 source 200 strategy replace

Switch(config)#

1.3.14 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

1.3.15 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

1.3.16 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

1.3.17 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

1.3.18 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

1.3.19 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

1.3.20 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

1.3.21 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

1.3.22 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

1.3.23 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

1.3.24 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

1.4 Commands for IGMP Proxy

1.4.1 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

1.4.2 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

1.4.3 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

1.4.4 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

1.4.5 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

1.4.6 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

1.4.7 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

1.4.8 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

1.4.9 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

1.4.10 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

1.4.11 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

1.4.12 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

1.4.13 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

1.4.14 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

1.4.15 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

1.4.16 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

1.4.17 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

1.4.18 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

1.4.19 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)

1.4.20 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 Commands for IPv6 DCSCM

2.1.1 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

2.1.2 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

2.1.3 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)#

2.1.4 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

2.1.5 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

2.1.6 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

2.1.7 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

2.1.8 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

2.1.9 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

2.1.10 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)#

2.1.11 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

2.1.12 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

2.1.13 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

2.1.14 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

2.2 Commands for MLD

2.2.1 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

2.2.2 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

2.2.3 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

2.2.4 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

2.2.5 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

2.2.6 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

2.2.7 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

2.2.8 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

2.2.9 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

2.2.10 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

2.2.11 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

2.2.12 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

2.2.13 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

2.2.14 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 is routers still not upgraded to version 2 of MLD protocol on the subnet connected, the interface should be configured to corresponding version.
Example: Configure the MLD version to 2.
Swith(config)#interface vlan 1
Swith(config-if-vlan1)#ipv6 mld version 2

2.2.15 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

2.2.16 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

2.2.17 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

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 multicast-vlan mode

Command: multicast-vlan mode {dynamic| compatible}
no multicast-vlan mode {dynamic| compatible}

Function: This command is used to configure the two modes of the multicast vlan; the no command cancels this configuration.

Parameters: dynamic: dynamic mode;
compatible: compatible mode.

Command mode: VLAN configuration mode.

Default: Neither of the two modes.

Usage Guide: When configured as dynamic mode, the mrouter port will not be added automatically any mort when issuing the multicast entries; when configured as

compatible mode, the report packet will be not transmitted to the mrouter port any more. When it is not configured as default, the mrouter port will be added when issuing the multicast entries and the report packet will be transmitted to the mrouter port when it is received.

Example:

Switch(Config-Vlan2)#multicast vlan mode dynamic
Switch(Config-Vlan2)#

3.5 switchport association multicast-vlan

Command: switchport association multicast-vlan <*vlan-id*> out-tag <*tag-id*>
no switchport association multicast-vlan <*vlan-id*>

Function: Associate a port with the specified multicast VLAN; the no command cancels the association.

Parameter: <*vlan-id*>: The multicast VLAN associates with the port. Each port can only be associated with one multicast VLAN, and the association will be successful only when the multicast VLAN is existent.

<*tag-id*>: Specify vlan tag of the multicast data forwarded by the associated port, only the tag of the associated port allows the multicast VLAN, the tag-id takes effect. Its range from 1 to 4094.

Command Mode: Port mode.

Default: The port is not associated with any multicast VLAN by default.

Usage Guide: After a port is associated with the multicast VLAN, when there comes the multicast order in the port, then the multicast data will be sent from the multicast VLAN to this port, so to reduce the data traffic. If the associated port is set as trunk port and allows the multicast VLAN, the multicast traffic with the specified vlan tag will be forwarded. The port can only be associated with the multicast VLAN after the multicast VLAN is enabled.

Example:

Switch(config)#vlan 2
Switch(Config-Vlan2)#multicast-vlan
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#switchport mode trunk
Switch(config-if-ethernet1/0/1)#switchport association multicast-vlan 2 out-tag 5