Content

Chapter 1 IPv4 Multicast Protocol

1.1 Commands for DCSCM

1.1.1 access-list (Multicast Destination Control)

Command: **access-list <6000-7999> {{{add | delete} profile-id WORD} | {{deny| permit} (ip) {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination}}**

no access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip> {range <2-65535>|}}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip> {range <2-255>|}}|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.

{add | delete}: add or delete the profile.

{deny|permit}: deny or permit.

<source/M>: multicast source address and mask length.

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

<2-65535>: the range of multicast source host.

<destination/M>: multicast destination address and mask length.

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

<2-255>: the range of multicast destination host.

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 ip 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 mask length 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. And adding or deleting the profile-id can be used to change the multicast destination control ACL.

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

1.1.2 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

1.1.3 ip multicast destination-control

This command is not supported by the switch.

1.1.4 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)#

1.1.5 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

1.1.6 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

1.1.7 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

1.1.8 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

1.1.9 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

1.1.10 multicast destination-control

Command: multicast destination-control
no multicast destination-control
Function: Configure to globally enable multicast destination control, the NO command is

to recover and disable the 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

1.1.11 profile-id (Multicast Destination Control Rule List)

Command: profile-id <1-50> {deny|permit} {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination}

no profile-id <1-50>

Function: Configure the destination control profile rule. The no command deletes the profile rule.

Parameters: <1-50>: profile-id.

{deny|permit}: deny or permit.

<source/M>: multicast source address and mask length.

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

<2-65535>: range of multicast source host.

<destination/M>: multicast destination address and mask length.

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

<2-255>: range of multicast destination host.

Default: None.

Command Mode: Global Mode.

Usage Guide: Profile-list of Multicast destination control list item is controlled by specifical profile-id number from 1 to 50, the command applies to configure this profile to add it into the ACL for using. 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 ACLs, and use mask length 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)# profile-id 1 deny ip any-source host-destination 224.1.1.2

1.1.12 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)#

1.1.13 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

1.1.14 show ip multicast destination-control filter-profile-list

Command: show ip multicast destination-control filter-profile-list
show ip multicast destination-control filter-profile-list <1-50>
Function: Show the configured destination control profile rule list.
Parameters: <1-50>: profile-id.
Default: None.
Command Mode: Admin and configuration mode.
Usage Guide: This command can show the configured destination control profile rule list.
Example:
Switch#show ip multicast destination-control filter-profile-list
profile-id 1 deny ip any-source any-destination
profile-id 2 deny ip any-source host-destination 224.1.1.1
profile-id 3 deny ip host-source 2.1.1.1 any-destination

1.1.15 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

1.1.16 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

1.1.17 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

1.2 Commands for IGMP Snooping

1.2.1 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>

1.2.2 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

1.2.3 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".

1.2.4 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

1.2.5 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

1.2.6 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

1.2.7 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

1.2.8 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

1.2.9 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

1.2.10 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

1.2.11 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

1.2.12 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

1.2.13 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)#

1.2.14 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

1.2.15 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

1.2.16 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

1.2.17 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

1.2.18 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

1.2.19 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

1.2.20 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

1.2.21 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

1.2.22 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

1.2.23 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

1.2.24 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	Whether the VLAN enables l2-general-querier function

querier	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

1.3 Commands for IGMP Snooping Authentication

1.3.1 igmp snooping authentication enable

Command: igmp snooping authentication enable
no igmp snooping authentication enable
Function: Configure the port of the switch as the igmp authentication port. After the successful configuration, the switch has the igmp authentication function in this port. The no command disables this function.
Command Mode: Port Mode.
Default: Disable.
Usage Guide: If the switch should conduct authentication for the multicast group of client demanding, use this command to configure the port. The ports without configuring this command will not conduct authentication for the demanded packet.
Example: Enable the IGMP authentication function on the port.
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#igmp snooping authentication enable

1.3.2 igmp snooping authentication free-rule access-list <6000-7999>

Command: igmp snooping authentication free-rule access-list <6000-7999>
no igmp snooping authentication free-rule access-list <6000-7999>
Function: Configure the authentication free-rule access list of the multicast group. The no command deletes it.

Parameters: <6000-7999>: number of access list.
Command Mode: Port Mode.
Default: Do not configure.
Usage Guide: This command can be effective only after the port authentication function is enabled. After configured this command, the multicast group of client demanding that the port received will be matched according to the configured access list. If it is permit, this multicast group is free for authentication and the table entry will be issued directly. Otherwise, it needs to conduct authentication.
Example: Configure the authentication free-rule access list of the multicast group.
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#igmp snooping authentication free-rule access-list 6000

1.3.3 ip igmp snooping authentication radius none

Command: ip igmp snooping authentication radius none
no ip igmp snooping authentication radius none
Function: Configure the switch to work with successful authentication when the radius server has no response. The no command recovers the default authentication method, the switch works with failed authentication.
Command Mode: Global Mode.
Default: Adopt radius authentication, the server has no response, the switch works with failed authentication.
Example:
Switch(config)#ip igmp snooping authentication radius none

1.3.4 ip igmp snooping authentication forwarding-first

Command: ip igmp snooping authentication forwarding-first
no ip igmp snooping authentication forwarding-first
Function: Configure the process procedure of igmp authentication: issue the multicast table entry to the multicast group of client demanding and then conduct authentication. After the authentication is successful, there is no action, if the authentication failed, the issued table entry will be deleted. The no command recovers to be the default method: conducts the authentication first, and issues the table entry after the authentication result is back.
Command Mode: Global Mode.
Default: Conducts the authentication first, and issues the table entry after the authentication result is back.
Example:
Switch(config)#ip igmp snooping authentication forwarding-first

1.3.5 ip igmp snooping authentication timeout <30-30000>

Command: ip igmp snooping authentication timeout <30-30000>
no ip igmp snooping authentication timeout

Function: Configure the timeout of the table entry in igmp authentication, including permit and deny. When the timer is timeout, deletes all the authenticated entries of permit and deny. The no command recovers to be the default value.

Parameters: <30-30000>: timeout, unit is second.

Command Mode: Global Mode.

Default: 600 seconds.

Usage Guide: The switch records the authentication result for multicast group of client demanding into the table entry, including permit and deny rules. Before each authentication, checks the rule in the entry first. If the rule is found, there is no need for authentication and the authentication result can be used directly. Otherwise, sends authentication. It can reduce the times of authentication. But the configuration on radius server may be changed. The recorded authentication table entry results may be timeout, so they should be cleared. This command configures the global timeout.

Example: Configure the authenticationtable entry timeout.

Switch(config)#ip igmp snooping authentication timeout 30000

1.3.6 clear ip igmp snooping vlan <1-4094> groups (A.B.C.D|) ((authentication-port (ethernet IFNAME | IFNAME)) |)

Command: clear ip igmp snooping vlan <1-4094> groups (A.B.C.D|) ((authentication-port (ethernet IFNAME | IFNAME)) |)

Function: Force the user to get off the line, and clear the corresponding authentication record and issued table entry.

Parameters: <1-4094> is the appointed VLAN ID; A.B.C.D is the appointed group address; ethernet is the Ethernet name; IFNAME is the port name.

Command Mode: Admin Mode.

Usage Guide: Delete the group authentication record and the issued table entry quickly. The show command can be used to view the group record and authentication record.

Example:

Switch#clear ip igmp snooping vlan 1 groups 225.2.2.2 authentication-port ethernet 1/0/1

Related Command: show ip igmp snooping vlan <1-4094> groups (A.B.C.D|) (authentication-table |)

1.3.7 show ip igmp snooping vlan <1-4094> groups (A.B.C.D|) authentication-table

Command: show ip igmp snooping vlan <1-4094> groups (A.B.C.D|) authentication-table

Function: Show the authentication table entry record.

Parameters: <1-4094> is the appointed VLAN ID; A.B.C.D is the appointed group address.

Command Mode: Admin Mode.

Example:

Switch# config

Switch(config)# show ip igmp snooping vlan 1 groups 225.1.1.1 authentication-table

Igmp snooping authentication permit information for vlan 1 :

Igmp snooping authentication-table expire 00:09:56, 600

Vlan	Ports	Groups	Mac	AuthState
1	Ethernet1/0/11	225.1.1.1	F0-7D-68-FA-7E-F3	permit
1	Ethernet1/0/11	225.1.1.1	04-0A-EB-6A-7F-88	permit
1	Ethernet1/0/11	225.1.1.1	03-0A-EB-6A-7F-88	permit

1.3.8 show ip igmp snooping authentication free-rule ((interface (ethernet IFNAME|IFNAME))|)

Command: show ip igmp snooping authentication free-rule ((interface (ethernet IFNAME|IFNAME))|)

Function: Show the igmp free authentication rule configured on the port.

Parameters: ethernet is the Ethernet name; IFNAME is the port name.

Command Mode: Admin Mode.

Example:

Switch(config)#show ip igmp snooping authentication free-rule

access-list 6001 used on interface Ethernet1/0/1

access-list 6001 permit ip any-source 224.0.0.0 0.0.0.255

1.3.9 debug igmp snooping authentication (event| timer|all)

Command: debug igmp snooping authentication (event|timer|all)

no debug igmp snooping authentication (event|timer|all)

Function: Enable the debugging on-off of the IGMP Snooping authentication on the switch. The no command disables it.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: It is used to enable the debugging on-off of the IGMP Snooping authentication on the switch. It can show the information of event, timer and all (all the debugs) that the switch deals with the IGMP authentication.

Chapter 2 IPv6 Multicast Protocol

2.1 Commands for MLD Snooping Configuration

2.1.1 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>

2.1.2 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

2.1.3 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.

2.1.4 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

2.1.5 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

2.1.6 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

2.1.7 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

2.1.8 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

2.1.9 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

2.1.10 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

2.1.11 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

2.1.12 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

2.1.13 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

2.1.14 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

2.1.15 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

2.1.16 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

2.1.17 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 out-tag <*tag-id*>

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

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: 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 1/2
Switch(config-vlan2)#multicast-vlan association interface port-channel 2
Switch(config-vlan2)#no multicast-vlan association interface ethernet 1/2
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