QASA CLI GUIDE

Multicast Protocol

Contents

1. IPv4 Multicast

access-list (Multicast Destination Control)

Command	**access-list <6000-7999> (((add | delete) profile-id WORD) | ((deny | permit) ip ((<source> <wildcard-bit>) | (host-source <source-host-ip> [range <2-65535>]) | any-source) ((<destination> <wildcard-bit>) | (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)**
Parameter	**<6000-7999>:** destination control access-list number. **add | delete:** add or delete the profile **WORD:** File id **deny | permit:** deny or permit **<source>:** multicast source address **<wildcard-bit>:** Address wildcard **<source-host-ip>:** multicast source host address. **<2-65535>:** the range of multicast source host. **<destination>:** multicast destination address **<destination-host-ip>:** multicast destination host address **<2-255>:** the range of multicast destination host.
Default	None.
Mode	Global mode.
Usage	ACL of Multicast destination control list item is controlled by specifically 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** **Switch(config)#access-list 6000 permit ip 10.1.1.1 0.0.0.255 232.0.0.0 0.0.0.255**

access-list (Multicast Source Control)

Command	**access-list <5000-5099> (deny | permit) ip ((<source> <wildcard-bit>) | (host <source-host-ip>) | any-source) ((<destination> <wildcard-bit>) | (host-destination <destination-host-ip>) | any-destination}** **no access-list <5000-5099> (deny | permit) ip ((<source> <wildcard-bit>) | (host <source-host-ip>) | any-source) ((<destination> <wildcard-bit>) | (host-destination <destination-host-ip>) | any-destination)**
Parameter	**<5000-5099>:** source control access-list number **deny | permit:** deny or permit. **<source>:** multicast source address. **<wildcard-bit>:** address wildcard character. **<source-host-ip>:** multicast source host address. **<destination>:** multicast destination address. **<destination-host-ip>:** multicast destination host address.
Default	None.
Mode	Global Mode.
Usage	ACL of Multicast source control list item is controlled by specifically 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**

ip multicast destination-control access-group

Command	**ip multicast destination-control access-group <6000-7999>** **no ip multicast destination-control access-group <6000-7999>**
Parameter	**<6000-7999>:** destination-control access-list number.
Default	None.
Mode	Interface Configuration Mode.
Usage	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** **Switch(config)#interface ethernet 1/0/4** **Switch(config-if-ethernet1/0/4)#ip multicast destination-control access-group 6000**

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>**
Parameter	**<IPADDRESS/M>:** IP address and mask length **<6000-7999>:** Destination control access-list number
Default	None.
Mode	Global Mode.
Usage	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** **Switch(config)#ip multicast destination-control 10.1.1.0/24 access-group 6000**

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>**
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.
Mode	Global Mode.
Usage	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** **Switch(config)#ip multicast destination-control 1 00-01-03-05-07-09 access-group 6000**

ip multicast policy

Command	**ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>** **no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos**
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.
Mode	Global Mode.
Usage	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**

ip multicast source-control

Command	**ip multicast source-control** **no ip multicast source-control**
Parameter	None.
Default	Disabled.
Mode	Global Mode.

Usage	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**

ip multicast source-control access-group

Command	**ip multicast source-control access-group <5000-5099>** **no ip multicast source-control access-group <5000-5099>**
Parameter	**<5000-5099>:** Source control access-list number.
Default	None.
Mode	Interface Configuration Mode.
Usage	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**

ip multicast destination-control

Command	**ip multicast destination-control**
Parameter	None.
Default	Disabled.
Mode	Global Mode.
Usage	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)#ip multicast destination-control**

profile-id (Multicast Destination Control Rule List)

Command	**profile-id <1-50> (deny | permit) ip ((<source> <wildcard-bit>) | (host-source <source-host-ip> [range <2-65535>]) | any-source} ((<destination> <wildcard-bit>) | (host-destination <destination-host-ip> [range <2-255>]) | any-destination)** **no profile-id <1-50>**
Parameter	**<1-50>:** profile-id **deny | permit:** deny or permit. **<source>:** multicast source address. **<wildcard-bit>:** address wildcard character. **<source-host-ip>:** multicast source host address. **<2-65535>:** range of multicast source host. **<destination>:** multicast destination address. **<destination-host-ip>:** multicast destination host address. **<2-255>:** range of multicast destination host.
Default	None.
Mode	Global Mode.
Usage	Profile-list of Multicast destination control list item is controlled by specifically 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**

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]**
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.

	<ipaddress>: IP address **<vlan-id>:** VLAN ID **<mac-address>:** Mac address
Default	None.
Mode	Admin Mode and Global Mode.
Usage	The command displays multicast destination control rules of configuration including detail option, and access-list information applied in detail.
Example	**Switch#show ip multicast destination-control** ip multicast destination-control is enabled multicast destination-control access-group 6000 used on interface Ethernet1/0/4

show ip multicast destination-control access-list

Command	**show ip multicast destination-control access-list**
Parameter	**<1-50>:** profile-id
Default	None.
Mode	Admin Mode and Global Mode.
Usage	This command can show the configured destination control profile rule list.
Example	**Switch#show ip multicast destination-control access-list**

show ip multicast policy

Command	**show ip multicast policy**
Parameter	**None.**
Default	None.
Mode	Admin Mode and Global Mode.
Usage	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**

show ip multicast source-control

Command	**show ip multicast source-control [detail]** **show ip multicast source-control interface <Interfacename> [detail]**
Parameter	**detail**: expresses if it displays information in detail. **<Interfacename>:** interface name, such as ethernet 1/0/1 or ethernet1/0/1.
Default	None.
Mode	Admin Mode and Global Mode.
Usage	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

show ip multicast source-control access-list

Command	**show ip multicast source-control access-list** **show ip multicast source-control access-list <5000-5099>**
Parameter	**<5000-5099>:** access-list number
Default	None.
Mode	Admin Mode and Global Mode.
Usage	The command displays source control multicast access-list of configuration.
Example	**Switch#show 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

clear ip igmp snooping vlan

Command	**clear ip igmp snooping vlan <1-4094> groups [A.B.C.D]**
Parameter	**<1-4094>:** VLAN ID **[A.B.C.D]:** group address.
Default	None.
Mode	Admin Mode and Global Mode.
Usage	Use show command to check the deleted group record.
Example	**Switch#clear ip igmp snooping vlan 1 groups**

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

Command	**clear ip igmp snooping vlan <1-4094> mrouter-port [ethernet] IFNAME**
Parameter	**<1-4094>:** VLAN ID **IFNAME**: port name
Default	None.
Mode	Admin Configuration Mode.
Usage	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**

ip igmp snooping

Command	**ip igmp snooping** **no ip igmp snooping**
Parameter	None.
Default	IGMP Snooping is disabled by default.
Mode	Admin Configuration Mode.
Usage	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** **Switch(config)#ip igmp snooping**

ip igmp snooping proxy

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

ip igmp snooping vlan

Command	**ip igmp snooping vlan <vlan-id>** **no ip igmp snooping vlan <vlan-id>**
Parameter	**<vlan-id>:** VLAN ID
Default	IGMP Snooping is disabled by default.
Mode	Global Mode.
Usage	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** **Switch(config)#ip igmp snooping vlan 100**

ip igmp snooping vlan immediate-leave

Command	**ip igmp snooping vlan <vlan-id> immediate-leave** **no ip igmp snooping vlan <vlan-id> immediate-leave**
Parameter	**<vlan-id>:** VLAN ID
Default	This function is disabled by default.
Mode	Global Mode.
Usage	Enables 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** **Switch(config)#ip igmp snooping vlan 100 immediate-leave**

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

Command	**ip igmp snooping vlan <vlan-id> immediately-leave mac-based** **no ip igmp snooping vlan <vlan-id> immediately-leave mac-based**
Parameter	**<vlan-id>:** VLAN ID
Default	This function is disabled by default.
Mode	Global Mode.
Usage	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. 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 **Switch(config)#ip igmp snooping vlan 12 immediately-leave** **Switch(config)#ip igmp snooping vlan 12 immediately-leave mac-based**

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**
Parameter	**<vlan-id>:** is ID number of the VLAN, ranging is <1-4094>.
Default	VLAN is not as the IGMP Snooping layer 2 general querier.
Mode	Global Mode.
Usage	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
Example	**Switch(config)#ip igmp snooping vlan 1 l2-general-querier**

ip igmp snooping vlan l2-general-querier-source

Command	**ip igmp snooping vlan <vlanid> l2-general-querier-source A.B.C.D <ipaddress>**
Parameter	**<vlan-id>:** VLAN ID **<version>:** version number, limited to <1-3>.
Default	version 3.
Mode	Global Mode.
Usage	This command is used to set the querier source ip address
Example	**Switch(config)#ip igmp snooping vlan 100 l2-general-querier-source 224.1.1.2**

ip igmp snooping vlan l2-general-querier-version

Command	**ip igmp snooping vlan <vlanid> l2-general-querier-version <version>**
Parameter	**<vlan-id>:** VLAN ID **<version>:** version number, limited to <1-3>.
Default	version 3.
Mode	Global Mode.
Usage	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-querier-version 2**

ip igmp snooping vlan limit

Command	**ip igmp snooping vlan <vlanid> limit {group <g_limit> | source <s_limit>}** **no ip igmp snooping vlan <vlan-id> limit**
Parameter	**<vlan-id>:** VLAN ID **<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.
Default	Maximum 50 groups by default, with each group capable with 40 source entries.
Mode	Global Mode.
Usage	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**

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

Command	**ip igmp snooping vlan <vlanid> interface (ethernet | port-channel) IFNAME limit {group <g_limit> | source <s_limit>} strategy (replace | drop)** **no ip igmp snooping vlan <1-4094> interface (ethernet | port-channel) IFNAME limit group source strategy**
Parameter	**<vlan-id>:** VLAN ID **IFNAME**: Interface name **<g_limit>:** <1-65535>, The maximum number of groups allowed joining **<s_limit>:** <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.
Default	There is no limitation as default.
Mode	Global Mode.
Usage	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**

ip igmp snooping vlan mrouter-port interface

Command	**ip igmp snooping vlan <vlanid> mrouter-port interface [ehternet | port-channel] <ifname>** **no ip igmp snooping vlan <vlan-id> mrouter-port interface[<ehternet> | <port-channel>] <ifname>**
Parameter	**<vlan-id>:** VLAN ID **IFNAME**: Name of interface.
Default	No static mrouter port on VLAN by default.
Mode	Global Mode.
Usage	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**

ip igmp snooping vlan mrouter-port learnpim

Command	**ip igmp snooping vlan <vlanid> mrouter-port learnpim** **no ip igmp snooping vlan <vlan-id> mrouter-port learnpim**
Parameter	**<vlan-id>:** VLAN ID
Default	Enable.
Mode	Global Mode.
Usage	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)#ip igmp snooping vlan 100 mrouter-port learnpim**

ip igmp snooping vlan mrpt

Command	**ip igmp snooping vlan <vlanid> mrpt <value>** **no ip igmp snooping vlan <vlan-id> mrpt**
Parameter	**<vlan-id>:** VLAN ID, ranging between <1-4094> **<value>:** mrouter port survive period, ranging between <1-65535>seconds
Default	255s.
Mode	Global Mode.
Usage	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**

ip igmp snooping vlan query-interval

Command	**ip igmp snooping vlan <vlanid> query-interval <*value*>** **no ip igmp snooping vlan <*vlan-id*> query-interval**
Parameter	**<vlan-id>:** VLAN ID, ranging between <1-4094> **<value>:** query interval, ranging between <1-65535>seconds.
Default	125s.
Mode	Global Mode.
Usage	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**

ip igmp snooping vlan query-mrsp

Command	**ip igmp snooping vlan <vlanid> query-mrsp <*value*>** **no ip igmp snooping vlan <*vlan-id*> query-mrspt**
Parameter	**<vlan-id>:** VLAN ID, ranging between <1-4094> **<value>:** ranging between <1-25> seconds
Default	10s.
Mode	Global Mode.
Usage	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**

ip igmp snooping vlan query-robustness

Command	**ip igmp snooping vlan <vlanid> query-robustness <value>** **no ip igmp snooping vlan <vlan-id> query-robustness**
Parameter	**<vlan-id>:** VLAN ID **<value>:** ranging between <2-10>
Default	2s.
Mode	Global Mode.

Usage	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**

ip igmp snooping vlan report source-address

Command	**ip igmp snooping vlan <vlanid> report source-address <A.B.C.D>** **no ip igmp snooping vlan <vlan-id> report source-address**
Parameter	**<vlan-id>:** VLAN ID **<value>:** IP address, can be 0.0.0.0
Default	Disabled.
Mode	Global Mode.
Usage	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**

ip igmp snooping vlan specific-query-mrsp

Command	**ip igmp snooping vlan <vlanid> specific-query-mrsp <value>** **no ip igmp snooping vlan <vlan-id> specific-query-mrspt**
Parameter	**<vlan-id>:** 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.
Default	Enable.
Mode	Global Mode.
Usage	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. **Switch(config)#ip igmp snooping vlan 3 specific-query-mrsp 2**

ip igmp snooping vlan static-group

Command	**ip igmp snooping vlan <vlanid> 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>**
Parameter	**<vlan-id>:** VLAN ID, ranging between <1-4094> **<A.B.C.D>:** address of group or source. **<IFNAME>:** Name of interface.
Default	None.
Mode	Global Mode.
Usage	Configures static-group on specified port of the VLAN. The no form of the command cancels this configuration. 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**

ip igmp snooping vlan suppression-query-time

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

show ip igmp snooping

<table>
<tr><td>Command</td><td>show ip igmp snooping [vlan <vlan-id>]</td></tr>
<tr><td>Parameter</td><td><vlan-id>: VLAN ID</td></tr>
<tr><td>Default</td><td>None.</td></tr>
<tr><td>Mode</td><td>Admin Configuration Mode.</td></tr>
<tr><td>Usage</td><td>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.</td></tr>
<tr><td>Example</td><td>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

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

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</td></tr>
</table>

<table>
<tr><td></td><td>!Ethernet1/0/2

<table>
<tr><td>!Ethernet1/0/2Displayed Information</td><td>Explanation</td></tr>
<tr><td>Igmp snooping L2 general querier</td><td>Whether the VLAN enables l2-general-querier function and show whether the querier state is could-query or suppressed</td></tr>
<tr><td>Igmp snooping query-interval</td><td>Query interval of the VLAN</td></tr>
<tr><td>Igmp snooping max reponse time</td><td>Max response time of the VLAN</td></tr>
<tr><td>Igmp snooping robustness</td><td>IGMP Snooping robustness configured on the VLAN</td></tr>
<tr><td>Igmp snooping mrouter port keep-alive time</td><td>keep-alive time of dynamic mrouter of the VLAN</td></tr>
<tr><td>Igmp snooping query-suppression time</td><td>Suppression timeout of VLAN when as l2-general-querier</td></tr>
<tr><td>IGMP Snooping Connect Group Membership</td><td>Group membership of this VLAN, namely the correspondence between ports and (S,G)</td></tr>
<tr><td>Igmp snooping vlan 1 mrouter port</td><td>mrouter port of the VLAN, including both static and dynamic</td></tr>
</table></td></tr>
</table>

clear ipv6 mld snooping vlan

Command	**clear ipv6 mld snooping vlan <1-4094> groups [X:X::X:X]**
Parameter	**<1-4094>:** VLAN ID **[X:X::X:X]:** specific group address
Default	None.
Mode	Admin Configuration Mode.
Usage	Delete the group record of the specific VLAN. Use show command to check the deleted group record.
Example	Delete all groups. **Switch#clear ipv6 mld snooping vlan 1 groups**

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

Command	**clear ipv6 mld snooping vlan <1-4094> mrouter-port [ethernet] IFNAME**
Parameter	**<1-4094>:** VLAN ID **[X:X::X:X]:** port name
Default	None.
Mode	Admin Configuration Mode.
Usage	Delete the mrouter port of the specific VLAN. 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**

ipv6 mld snooping

Command	**ipv6 mld snooping** **no ipv6 mld snooping**
Parameter	None.
Default	MLD Snooping disabled on the switch by default.
Mode	Admin Configuration Mode.
Usage	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**

ipv6 mld snooping vlan

Command	**ipv6 mld snooping vlan <vlan-id>** **no ipv6 mld snooping vlan <vlan-id>**
Parameter	**<vlan-id>:** VLAN ID, with a valid range of <1-4094>.
Default	MLD Snooping disabled on the switch by default.
Mode	Admin Configuration Mode.

Usage	Enable MLD Snooping on specified VLAN; the "no" form of this command disables MLD Snooping on specified VLAN. 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**

ipv6 mld snooping vlan immediate-leave

Command	**ipv6 mld snooping vlan <vlan-id> immediate-leave** **no ipv6 mld snooping vlan <vlan-id> immediate-leave**
Parameter	**<vlan-id>:** VLAN ID, with valid range of <1-4094>.
Default	Disabled by default.
Mode	Global Mode.
Usage	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 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**

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**
Parameter	**<vlan-id>:** VLAN ID, with a valid range of <1-4094>.
Default	VLAN is not a MLD Snooping L2 general querier by default.
Mode	Global Mode.
Usage	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**

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**
Parameter	**<vlan-id>:** VLAN ID, with a valid range of <1-4094>. **<g_limit>:** max number of groups joined, range: 1-65535. **<s_limit>:** max number of source entries in each group, consisting of include source and exclude source, range: 1-65535.
Default	Maximum 50 groups by default, with each group capable with 40 source entries.
Mode	Global Mode.
Usage	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**

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>**
Parameter	**<vlan-id>:** VLAN ID,the valid range is<1-4094>. **<ifname>:** Name of interface
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.
Mode	Global Mode.
Usage	Sets the static mrouter port of the VLAN; the "no" form of this command cancels the configuration.
Example	**Switch(config)#ipv6 mld snooping vlan 2 mrouter-port interface ethernet1/0/13**

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**
Parameter	**<vlan-id>:** VLAN ID,the valid range is<1-4094>. **<ifname>:** Name of interface
Default	Enable.
Mode	Global Mode.
Usage	Enables 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)#ipv6 mld snooping vlan 2 mrouter-port learnpim6**

ipv6 mld snooping vlan mrpt

Command	**ipv6 mld snooping vlan <vlan-id> mrpt <value>** **no ipv6 mld snooping vlan <vlan-id> mrpt**
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.
Default	255s.
Mode	Global Mode.
Usage	Configures the keep-alive time of the mrouter port. 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**

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**
Parameter	**<vlan-id>:** VLAN ID, the valid range is <1-4094>. **<value>:** query interval, valid range: <1-65535>secs.
Default	125s.
Mode	Global Mode.
Usage	Configure the query interval. 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**

ipv6 mld snooping vlan query-mrsp

Command	**ipv6 mld snooping vlan <vlan-id> query-mrsp <value>** **no ipv6 mld snooping vlan <vlan-id> query-mrspt**
Parameter	**<vlan-id>:** VLAN ID, the valid range is <1-4094>. **<value>:** the valid range is <1-25> secs.
Default	10s.
Mode	Global Mode.
Usage	Configures the maximum query response period. The "no" form of this command restores the default value. 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**

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**
Parameter	**<vlan-id>:** VLAN ID,the valid range is <1-4094>. **<value>:** the valid range is <2-10>.
Default	2s.
Mode	Global Mode.
Usage	Configures the query robustness; the "no" form of this command restores to the default value. 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**

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>**
Parameter	**<vlan-id>:** VLAN ID,the valid range is <1-4094>. **<X:X::X:X>:** The address of group or source. **<IFNAME>:** Name of interface.
Default	None.
Mode	Global Mode.
Usage	Configures static-group on specified port of the VLAN. The no form of the command cancels this configuration. 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)#ipv6 mld snooping vlan 2 static-group ff1e::15 source 2000::1 interface ethernet 1/0/1**

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**
Parameter	**<vlan-id>:** VLAN ID, valid range: <1-4094>. **<value>:** valid range: <1-65535>secs.
Default	255s.
Mode	Global Mode.
Usage	Configures the suppression query time; the "no" form of this command restores the default value. 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**

show ipv6 mld snooping

<table>
<tr><td>Command</td><td>show ipv6 mld snooping [vlan <vlan-id>]</td></tr>
<tr><td>Parameter</td><td><vlan-id>: VLAN ID</td></tr>
<tr><td>Default</td><td>None.</td></tr>
<tr><td>Mode</td><td>Admin Configuration Mode.</td></tr>
<tr><td>Usage</td><td>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.</td></tr>
<tr><td>Example</td><td>1.Summary of the switch MLD snooping
Switch#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

<table>
<tr><td>Displayed Information</td><td>Explanation</td></tr>
<tr><td>Global mld snooping status</td><td>Whether or not the global MLD Snooping is enabled on the switch</td></tr>
<tr><td>L3 multicasting</td><td>Whether or not the layer 3 multicast protocol is running on the switch.</td></tr>
<tr><td>Mld snooping is turned on for vlan 1(querier)</td><td>On which VLAN of the switch is enabled MLD Snooping, if the VLAN are l2-general-querier.</td></tr>
</table>

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</td></tr>
</table>

<table>
<tr><td></td><td>Mld snooping vlan 1 mrouter port
Note:"!"-static mrouter port
!Ethernet1/0/2
<table><tr><th>Displayed Information</th><th>Explanation</th></tr><tr><td>Mld snooping L2 general querier</td><td>whether or not l2-general-querier is enabled on VLAN, the querier display status is set to could-query or suppressed</td></tr><tr><td>Mld snooping query-interval</td><td>Query interval time of the VLAN</td></tr><tr><td>Mld snooping max reponse time</td><td>Max response time of this VLAN</td></tr><tr><td>Mld snooping robustness</td><td>Robustness configured on the VLAN</td></tr><tr><td>Mld snooping mrouter port keep-alive time</td><td>Keep-alive time of the dynamic mrouter on this VLAN</td></tr><tr><td>Mld snooping query-suppression time</td><td>Timeout of the VLAN as l2-general-querier at suppressed status.</td></tr><tr><td>MLD Snooping Connect Group Membership</td><td>Group membership of the VLAN, namely the correspondence between the port and （S,G）</td></tr><tr><td>Mld snooping vlan 1 mrouter port</td><td>Mrouter port of the VLAN, including both static and dynamic.</td></tr></table></td></tr>
</table>

multicast-vlan

Command	**multicast-vlan** **no multicast-vlan**
Parameter	None.
Default	Multicast VLAN function not enabled by default.
Mode	VLAN Configuration Mode.
Usage	Enable multicast VLAN function on a VLAN; the “no” form of this command disables the multicast VLAN function. The multicast VLAN function cannot 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 cannot be configured with this command and only one multicast VLAN is allowed on a switch.
Example	**Switch(config)#vlan 2** **Switch(config-vlan2)# multicast-vlan**

multicast-vlan association

Command	**multicast-vlan association <vlan-list>** **no multicast-vlan association <vlan-list>**
Parameter	**<vlan-list>:** *<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.
Default	The multicast VLAN is not associated with any VLAN by default.
Mode	VLAN Configuration Mode.
Usage	Associate several VLANs with a multicast VLAN; the "no" form of this command cancels the association relations. 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.
Example	**Switch(config)#vlan 2** **Switch(config-vlan2)# multicast-vlan association 3, 4**

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**
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.
Default	None.
Mode	VLAN Configuration Mode.
Usage	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. 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	**Switch(config)#vlan 2** **Switch(config-vlan2)# multicast-vlan association interface ethernet 1/0/2** **Switch(config-vlan2)#multicast-vlan association interface port-channel 2**

multicast-vlan mode

Command	**multicast-vlan mode {dynamic | compatible}** **no multicast-vlan mode {dynamic | compatible}**
Parameter	**dynamic**: dynamic mode **compatible:** compatible mode
Default	Neither of the two modes.
Mode	VLAN Configuration Mode.
Usage	This command is used to configure the two modes of the multicast vlan; the no command cancels this configuration. 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)#vlan 2** **Switch(config-vlan2)# multicast-vlan mode dynamic**

switchport association multicast-vlan

Command	**switchport association multicast-vlan <vlan-id> out-tag <tag-id>** **no switchport association multicast-vlan <vlan-id>**
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.
Default	The port is not associated with any multicast VLAN by default.
Mode	Interface Configuration Mode.
Usage	Associates a port with the specified multicast VLAN; the no command cancels the association. 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**