

Contents

IGMP snooping commands	1
display igmp-snooping	1
display igmp-snooping group	3
display igmp-snooping host-tracking	5
display igmp-snooping router-port	6
display igmp-snooping static-group	7
display igmp-snooping static-router-port	8
display igmp-snooping statistics	9
display l2-multicast fast-forwarding cache	10
display l2-multicast ip	12
display l2-multicast ip forwarding	13
display l2-multicast mac	14
display l2-multicast mac forwarding	15
display mac-address [multicast]	16
dot1p-priority (IGMP-snooping view)	17
dscp	18
enable (IGMP-snooping view)	18
entry-limit (IGMP-snooping view)	19
fast-leave (IGMP-snooping view)	20
global-enable (IGMP-snooping view)	20
group-policy (IGMP-snooping view)	21
host-aging-time (IGMP-snooping view)	22
host-tracking (IGMP-snooping view)	23
igmp-snooping	24
igmp-snooping access-policy	24
igmp-snooping dot1p-priority	25
igmp-snooping drop-unknown	26
igmp-snooping { disable enable }	27
igmp-snooping fast-leave	28
igmp-snooping general-query source-ip	29
igmp-snooping group-limit	29
igmp-snooping group-policy	30
igmp-snooping host-aging-time	31
igmp-snooping host-join	32
igmp-snooping host-tracking	33
igmp-snooping last-member-query-interval	34
igmp-snooping leave source-ip	35
igmp-snooping max-response-time	36
igmp-snooping overflow-replace	37
igmp-snooping proxy enable	37
igmp-snooping querier	38
igmp-snooping querier-election	39
igmp-snooping query-interval	39
igmp-snooping report source-ip	40
igmp-snooping router-aging-time	41
igmp-snooping router-port-deny	42
igmp-snooping source-deny	43
igmp-snooping special-query source-ip	43
igmp-snooping static-group	44
igmp-snooping static-router-port	45
igmp-snooping version	46
last-member-query-interval (IGMP-snooping view)	46
mac-address multicast	47
max-response-time (IGMP-snooping view)	48
overflow-replace (IGMP-snooping view)	49
report-aggregation (IGMP-snooping view)	50
reset igmp-snooping group	50

reset igmp-snooping router-port.....	51
reset igmp-snooping statistics	51
reset l2-multicast fast-forwarding cache.....	52
router-aging-time (IGMP-snooping view)	52
source-deny (IGMP-snooping view).....	53
version (IGMP-snooping view)	54

IGMP snooping commands

display igmp-snooping

Use `display igmp-snooping` to display IGMP snooping status.

Syntax

```
display igmp-snooping [ global | vlan vlan-id ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

global: Displays the global IGMP snooping status.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

Usage guidelines

If you do not specify any parameters, this command displays the global IGMP snooping status and the IGMP snooping status in all VLANs.

Examples

Display the global IGMP snooping status and the IGMP snooping status for all VLANs.

```
<Sysname> display igmp-snooping
```

```
IGMP snooping information: Global
```

```
Global-enable: Enabled
```

```
Host-aging-time: 260s
```

```
Router-aging-time: 260s
```

```
Max-response-time: 10s
```

```
Last-member-query-interval: 1s
```

```
Report-aggregation: Enabled
```

```
Host-tracking: Disabled
```

```
Dot1p-priority: --
```

```
IGMP snooping information: VLAN 1
```

```
IGMP snooping: Enabled
```

```
Drop-unknown: Disabled
```

```
Version: 2
```

```
Host-aging-time: 260s
```

```
Router-aging-time: 260s
```

```
Max-response-time: 10s
```

```
Last-member-query-interval: 1s
```

```
Querier: Enabled (IP: 1.1.1.1, Expires: 00:02:05)
```

```
Querier-election: Enabled
```

```
Query-interval: 125s
```

```
General-query source IP: 1.1.1.1
```

Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Host-tracking: Disabled
 Dot1p-priority: 2
 Proxy: Disabled

IGMP snooping information: VLAN 10

IGMP snooping: Enabled
 Drop-unknown: Enabled
 Version: 3
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Enabled (IP: 1.1.1.1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
 Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Host-tracking: Disabled
 Dot1p-priority: --
 Proxy: Disabled

Table 1 Command output

Field	Description
Global-enable	Global IGMP snooping status: <ul style="list-style-type: none"> • Enabled. • Disabled.
IGMP snooping	IGMP snooping status in a VLAN: <ul style="list-style-type: none"> • Enabled. • Disabled. • Globally enabled. • Inactive—IGMP snooping configuration does not take effect.
Drop-unknown	Status of dropping unknown multicast data: <ul style="list-style-type: none"> • Enabled. • Disabled.
Version	IGMP snooping version.
Host-aging-time	Aging timer for the dynamic member port.
Router-aging-time	Aging timer for the dynamic router port.
Max-response-time	Maximum response time for IGMP general queries.
Last-member-query-interval	Interval for sending IGMP group-specific queries.
Report-aggregation	Status of IGMP report suppression: <ul style="list-style-type: none"> • Enabled.

Field	Description
	<ul style="list-style-type: none"> Disabled.
Dot1p-priority	802.1p priority for IGMP messages. If the priority is not configured, this field displays two hyphens (--).
Querier	Status of IGMP snooping querier: <ul style="list-style-type: none"> Enabled. Disabled.
(IP: 1.1.1.1, Expires: 00:02:05)	IGMP snooping querier information: <ul style="list-style-type: none"> IP—IP address of the IGMP snooping querier. Expire—Remaining aging time for the IGMP snooping querier. This field is not displayed if IGMP snooping querier election is disabled.
Querier-election	Status of IGMP snooping querier election: <ul style="list-style-type: none"> Enabled. Disabled.
Query-interval	Interval for sending IGMP general queries.
General-query source IP	Source IP address of IGMP general queries.
Special-query source IP	Source IP address of IGMP group-specific queries.
Report source IP	Source IP address of IGMP reports.
Leave source IP	Source IP address of IGMP leave messages.
Host-tracking	Status of host tracking: <ul style="list-style-type: none"> Enabled Disabled. Globally enabled.
Proxy	Status of IGMP snooping proxying: <ul style="list-style-type: none"> Enabled. Disabled.

display igmp-snooping group

Use `display igmp-snooping group` to display information about dynamic IGMP snooping group entries.

Syntax

```
display igmp-snooping group [ group-address | source-address ] * [ vlan
vlan-id ] [ interface interface-type interface-number | [ verbose ] [ slot
slot-number ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information about dynamic IGMP snooping group entries for all multicast groups.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about dynamic IGMP snooping group entries for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about dynamic IGMP snooping group entries for all VLANs.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays brief information about dynamic IGMP snooping group entries for all interfaces.

verbose: Displays detailed information about dynamic IGMP snooping group entries. If you do not specify this keyword, the command displays brief information about dynamic IGMP snooping group entries.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about dynamic IGMP snooping group entries for the master device.

Examples

Display brief information about dynamic IGMP snooping group entries for GigabitEthernet 1/0/1.

```
<Sysname> display igmp-snooping group interface gigabitethernet 1/0/1
Total 1 entries.
```

```
GE1/0/1:
```

```
  VLAN 2: Total 1 entries.
    (0.0.0.0, 224.1.1.1)                (00:03:23)
```

Display detailed information about dynamic IGMP snooping group entries for VLAN 2.

```
<Sysname> display igmp-snooping group vlan 2 verbose
Total 1 entries.
```

```
VLAN 2: Total 1 entries.
```

```
(0.0.0.0, 224.1.1.1)
  Attribute: local port
  FSM information: dummy
  Host slots (0 in total):
  Host ports (1 in total):
    GE1/0/2                            (00:03:23)
```

Table 2 Command output

Field	Description
Total 1 entries	Total number of dynamic IGMP snooping group entries.
VLAN 2: Total 1 entries	Total number of dynamic IGMP snooping group entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where 0.0.0.0 in the S position means all multicast sources.
Attribute	Entry attribute: <ul style="list-style-type: none">• global port—The entry has a global port.• local port—The entry has a port that resides on the member device

Field	Description
	<p>for which the information is displayed.</p> <ul style="list-style-type: none"> • slot—The entry has ports that reside on other member devices except the member device for which the information is displayed.
FSM information	<p>Finite state machine information of the entry:</p> <ul style="list-style-type: none"> • delete—The entry attributes have been deleted. • dummy—The entry is a new temporary entry. • no info—No entry exists.
Host slots (0 in total)	Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports, and the total number of member ports.
(00:03:23)	<p>Remaining aging time for the dynamic member port.</p> <p>For a global port (such as Layer 2 aggregate interfaces), this field is always displayed.</p> <p>For a non-global port, this field is displayed when one of the following conditions exists:</p> <ul style="list-style-type: none"> • The port is on the specified member device. • The port is on the master device and no member device is specified.

Related commands

`reset igmp-snooping group`

display igmp-snooping host-tracking

Use `display igmp-snooping host-tracking` to display host tracking information.

Syntax

```
display igmp-snooping host-tracking vlan vlan-id group group-address
[ source source-address ] [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

group *group-address*: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255.

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays host tracking information for all multicast sources.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays host tracking information for the master device.

Examples

Display tracking information for hosts that have joined multicast group 224.1.1.1 in VLAN 2.

```
<Sysname> display igmp-snooping host-tracking vlan 2 group 224.1.1.1
```

```

VLAN 2
(0.0.0.0, 224.1.1.1)
Port: GE1/0/1
Host                Uptime             Expires
1.1.1.1             00:02:20          00:00:40
2.2.2.2             00:02:21          00:00:39

```

Table 3 Command output

Field	Description
VLAN	VLAN ID.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where 0.0.0.0 in the S position means any multicast sources.
Port	Member port.
Host	IP address of the host.
Uptime	Length of time elapsed since the host joined the multicast group.
Expires	Remaining timeout time for the host. The host timeout time is the same as the aging timer for the port. The timer is reset when the port receives an IGMP report from the host. This field displays timeout if the host times out.

Related commands

```

host-tracking (IGMP-snooping view)
igmp-snooping enable
igmp-snooping host-tracking

```

display igmp-snooping router-port

Use `display igmp-snooping router-port` to display dynamic router port information.

Syntax

```

display igmp-snooping router-port [ vlan vlan-id ] [ verbose ] [ slot
slot-number ]

```

Views

Any view

Predefined user roles

```

network-admin
network-operator

```

Parameters

verbose: Displays detailed information. If you do not specify the keyword, this command displays brief information.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays dynamic router port information for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays dynamic router port information for the master device.

Examples

```
# Display brief information about dynamic router ports for VLAN 2.
```

```
<Sysname> display igmp-snooping router-port vlan 2
```

```
VLAN 2:
```

```
Router ports (2 in total):
```

```
GE1/0/1 (00:01:30)
```

```
GE1/0/2 (00:00:23)
```

Table 4 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs and total number of the member devices that have dynamic router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Dynamic router ports and total number of dynamic router ports.
(00:01:30)	Remaining aging time for the dynamic router port. For a global port, this field is always displayed. For a global port, this field is displayed when one of the following conditions exists: <ul style="list-style-type: none">• The port is on the specified member device.• The port is on the master device and no member device is specified.

Related commands

```
reset igmp-snooping router-port
```

display igmp-snooping static-group

Use `display igmp-snooping static-group` to display information about static IGMP snooping group entries.

Syntax

```
display igmp-snooping static-group [ group-address | source-address ] *  
[ vlan vlan-id ] [ verbose ] [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-address: Specifies a multicast group by its IP address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays information about static IGMP snooping group entries for all multicast groups.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about static IGMP snooping group entries for all multicast sources.

vlan vlan-id: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about static IGMP snooping group entries for all VLANs.

verbose: Displays detailed information about static IGMP snooping group entries. If you do not specify the keyword, this command displays brief information about static IGMP snooping group entries.

slot slot-number: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about static IGMP snooping group entries for the master device.

Examples

Display detailed information about static IGMP snooping group entries for VLAN 2.

```
<Sysname> display igmp-snooping static-group vlan 2 verbose
Total 1 entries.
```

```
VLAN 2: Total 1 entries.
(0.0.0.0, 224.1.1.1)
Attribute: local port
FSM information: dummy
Host slots (0 in total):
Host ports (1 in total):
GE1/0/2
```

Table 5 Command output

Field	Description
Total 1 entries	Total number of static IGMP snooping group entries.
VLAN 2: Total 1 entries	Total number of static IGMP snooping group entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where 0.0.0.0 in the S position means all multicast sources.
Attribute	Entry attribute: <ul style="list-style-type: none"> global port—The entry has a global port. local port—The entry has a port that resides on the member device for which the information is displayed. slot—The entry has ports that reside on other member devices except the member device for which the information is displayed.
FSM information	Finite state machine information of the entry: <ul style="list-style-type: none"> delete—The entry attributes have been deleted. dummy—The entry is a new temporary entry. no info—No entry exists.
Host slots (0 in total)	Member IDs and total number of the member devices that have member ports, except for the specified member device or the master device when no member device is specified.
Host ports (1 in total)	Member ports and total number of member ports.

display igmp-snooping static-router-port

Use `display igmp-snooping static-router-port` to display static router port information.

Syntax

```
display igmp-snooping static-router-port [ vlan vlan-id ] [ verbose ] [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

verbose: Displays detailed information about static router ports. If you do not specify this keyword, the command displays brief information about static router ports.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays static router port information for the master device.

Examples

Display brief information about static router ports for VLAN 2.

```
<Sysname> display igmp-snooping static-router-port vlan 2
VLAN 2:
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

Display detailed information about static router ports for VLAN 2.

```
<Sysname> display igmp-snooping static-router-port vlan 2 verbose
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2
```

Table 6 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs and total number of the member devices that have static router ports, except for the specified member device or the master device when no member device is specified.
Router ports (2 in total)	Static router ports and total number of static router ports.

display igmp-snooping statistics

Use **display igmp-snooping statistics** to display statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping.

Syntax

```
display igmp-snooping statistics
```

Views

Any view

Predefined user roles

network-admin
network-operator

Examples

Display statistics for the IGMP messages and PIMv2 hello messages learned through IGMP snooping.

```
<Sysname> display igmp-snooping statistics
Received IGMP general queries: 0
Received IGMPv1 reports: 0
Received IGMPv2 reports: 19
Received IGMP leaves: 0
Received IGMPv2 specific queries: 0
Sent IGMPv2 specific queries: 0
Received IGMPv3 reports: 1
Received IGMPv3 reports with right and wrong records: 0
Received IGMPv3 specific queries: 0
Received IGMPv3 specific sg queries: 0
Sent IGMPv3 specific queries: 0
Sent IGMPv3 specific sg queries: 0
Received PIMv2 hello: 0
Received error IGMP messages: 19
```

Table 7 Command output

Field	Description
general queries	Number of IGMP general queries.
specific queries	Number of IGMP group-specific queries.
reports	Number of IGMP reports.
leaves	Number of IGMP leave messages.
reports with right and wrong records	Number of IGMP reports with correct and incorrect records.
specific sg queries	Number of IGMP group-and-source-specific queries.
PIMv2 hello	Number of PIMv2 hello messages.
error IGMP messages	Number of IGMP messages with errors.

Related commands

```
reset igmp-snooping statistics
```

display l2-multicast fast-forwarding cache

Use `display l2-multicast fast-forwarding cache` to display Layer 2 multicast fast forwarding entries.

Syntax

```
display l2-multicast fast-forwarding cache [ vlan vlan-id ]
[ source-address | group-address ] * [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

source-address: Specifies a multicast source address. If you do not specify a multicast source, this command displays Layer 2 multicast fast forwarding entries for all multicast sources.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255. If you do not specify a multicast group, this command displays Layer 2 multicast fast forwarding entries for all multicast groups.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 multicast fast forwarding entries for the master device.

Examples

Display Layer 2 multicast fast forwarding entries.

```
<Sysname> display l2-multicast fast-forwarding cache
```

```
Total 1 entries, 1 matched
```

```
(10.1.1.2, 225.1.1.1)
```

```
Status      : Enable          VLAN          : 1
Source port  : 9876           Destination port: 5432
Protocol     : 17            Flag          : 0x2
Ingress port: GigabitEthernet1/0/2
List of 1 egress ports:
  GigabitEthernet1/0/3
  Status: Enable          Flag: 0x10
```

Table 8 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries in the Layer 2 multicast fast forwarding table, and the total number of matching entries.
(10.1.1.2, 225.1.1.1)	(S, G) entry in the Layer 2 multicast fast forwarding table.
Protocol	Protocol number.
VLAN	VLAN ID.
Flag	Flag for the (S, G) entry or the outgoing port. This field displays one flag or the sum of multiple flags. In this example, the value 0x2 means that the entry has only one flag 0x2. The following flags are available for an entry: <ul style="list-style-type: none">• 0x1—The entry is created because of packets passed through between cards.• 0x2—The entry is added by multicast forwarding. The following flags are available for an outgoing interface: <ul style="list-style-type: none">• 0x1—The port is added to the entry because of packets passed through between cards.

Field	Description
	<ul style="list-style-type: none"> 0x2—The port is added to an existing entry. 0x10—The port is associated with the entry. 0x20—The port is to be deleted.
Status	Status of the (S, G) entry or the outgoing port: <ul style="list-style-type: none"> Enabled—Available. Disabled—Unavailable.
Ingress port	Incoming port of the (S, G) entry.
List of 1 egress ports	Outgoing port list of the (S, G) entry.

Related commands

```
reset l2-multicast fast-forwarding cache all
```

display l2-multicast ip

Use `display l2-multicast ip` to display information about Layer 2 IP multicast groups.

Syntax

```
display l2-multicast ip [ group group-address | source source-address ] *
[ vlan vlan-id ] [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

group *group-address*: Specifies a multicast group by its IP address. If you do not specify a multicast group, this command displays information about all Layer 2 IP multicast groups.

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays information about Layer 2 IP multicast groups for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 IP multicast groups for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 IP multicast groups for the master device.

Examples

Display information about Layer 2 IP multicast groups for VLAN 2.

```
<Sysname> display l2-multicast ip vlan 2
Total 1 entries.
```

```
VLAN 2: Total 1 entries.
(0.0.0.0, 224.1.1.1)
Attribute: static, success
Host ports (1 in total):
```

Table 9 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IP multicast groups.
VLAN 2: Total 1 entries	Total number of Layer 2 IP multicast groups in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where 0.0.0.0 in the S position means all multicast sources.
Attribute	Entry attribute: <ul style="list-style-type: none"> • dynamic—The entry is created by a dynamic protocol. • static—The entry is created by a static protocol. • pim—The entry is created by PIM. • kernel—The entry is obtained from the kernel. • success—Processing has succeeded. • fail—Processing has failed.
Host ports (1 in total)	Member ports and total number of member ports.
(S, SUC)	Port attribute: <ul style="list-style-type: none"> • D—Dynamic port. • S—Static port. • P—PIM port. • K—Port obtained from the kernel. • R—Port learned from (*, *) entries. • W—Port learned from (*, G) entries. • SUC—Processing has succeeded. • F—Processing has failed.

display l2-multicast ip forwarding

Use `display l2-multicast ip forwarding` to display Layer 2 multicast IP forwarding entries.

Syntax

```
display l2-multicast ip forwarding [ group group-address | source
source-address ] * [ vlan vlan-id ] [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *group-address*: Specifies a multicast group by its IP address. If you do not specify a multicast group, this command displays Layer 2 multicast IP forwarding entries for all multicast groups.

source *source-address*: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command displays Layer 2 multicast IP forwarding entries for all multicast sources.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 multicast IP forwarding entries for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 multicast IP forwarding entries for the master device.

Examples

Display Layer 2 multicast IP forwarding entries for VLAN 2.

```
<Sysname> display l2-multicast ip forwarding vlan 2  
Total 1 entries.
```

```
VLAN 2: Total 1 entries.  
  (0.0.0.0, 224.1.1.1)  
  Host ports (3 in total):  
    GigabitEthernet1/0/1  
    GigabitEthernet1/0/2  
    GigabitEthernet1/0/3
```

Table 10 Command output

Field	Description
Total 1 entries	Total number of Layer 2 multicast IP forwarding entries.
VLAN 2: Total 1 entries	Total number of Layer 2 multicast IP forwarding entries in VLAN 2.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where 0.0.0.0 in the S position means all multicast sources.
Host ports (3 in total)	Member ports and total number of member ports.

display l2-multicast mac

Use **display l2-multicast mac** to display information about Layer 2 MAC multicast groups.

Syntax

```
display l2-multicast mac [ mac-address ] [ vlan vlan-id ] [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

mac-address: Specifies a MAC multicast group by its multicast MAC address. If you do not specify a MAC multicast group, this command displays information about all Layer 2 MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays information about Layer 2 MAC multicast groups for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information about Layer 2 MAC multicast groups for the master device.

Examples

```
# Display information about Layer 2 MAC multicast groups for VLAN 2.
```

```
<Sysname> display l2-multicast mac vlan 2
```

```
Total 1 entries.
```

```
VLAN 2: Total 1 entries.
```

```
MAC group address: 0100-5e01-0101
```

```
Attribute: success
```

```
Host ports (1 in total):
```

```
GE1/0/1
```

Table 11 Command output

Field	Description
Total 1 entries	Total number of Layer 2 MAC multicast groups.
VLAN 2: Total 1 entries	Total number of Layer 2 MAC multicast groups in VLAN 2.
MAC group address	Address of the MAC multicast group.
Attribute	Entry attribute: <ul style="list-style-type: none">• success—Processing has succeeded.• fail—Processing has failed.
Host ports (1 in total)	Member ports and total number of member ports.

display l2-multicast mac forwarding

Use `display l2-multicast mac forwarding` to display Layer 2 multicast MAC forwarding entries.

Syntax

```
display l2-multicast mac forwarding [ mac-address ] [ vlan vlan-id ] [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies a MAC multicast group by its MAC address. If you do not specify a MAC multicast group, this command displays Layer 2 multicast MAC forwarding entries for all MAC multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays Layer 2 multicast MAC forwarding entries for all VLANs.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Layer 2 multicast MAC group entries for the master device.

Examples

```
# Display Layer 2 multicast MAC forwarding entries for VLAN 2.
```

```
<Sysname> display l2-multicast mac forwarding vlan 2
Total 1 entries.
```

```
VLAN 2: Total 1 entries.
  MAC group address: 0100-5e01-0101
  Host ports (3 in total):
    GigabitEthernet1/0/1
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3
```

Table 12 Command output

Field	Description
Total 1 entries	Total number of Layer 2 multicast MAC forwarding entries.
VLAN 2: Total 1 entries	Total number of Layer 2 multicast MAC forwarding entries in VLAN 2.
MAC group address	Address of the MAC multicast group.
Host ports (3 in total)	Member ports and total number of member ports.

display mac-address [multicast]

Use **display mac-address [multicast]** to display static multicast MAC address entries.

Syntax

```
display mac-address [ mac-address [ vlan vlan-id ] ] | [ multicast ] [ vlan vlan-id ] [ count ] ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

mac-address: Specifies a multicast MAC address. The MAC address can be any legal multicast MAC address except 0100-5Exx-xxxx and 3333-xxxx-xxxx, where "x" represents a hexadecimal number in the range of 0 to F.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command displays MAC address entries for all VLANs.

multicast: Specifies static multicast MAC address entries.

count: Specifies the number of MAC address entries. If you specify this keyword, the command displays the number of matching MAC address entries. If you do not specify this keyword, the command displays the contents of the matching entries rather than the entry count.

Usage guidelines

If you do not specify any parameters, this command displays all MAC address table entries, including unicast MAC address entries and static multicast MAC address entries.

Examples

```
# Display static multicast MAC address entries for VLAN 2.
```

```
<Sysname> display mac-address multicast vlan 2
MAC Address      VLAN ID   State      Port/NickName      Aging
0100-0001-0001  2         Multicast  GE1/0/1            N
```

Display the number of static multicast MAC address entries.

```
<Sysname> display mac-address multicast count
1 mac address(es) found.
```

Table 13 Command output

Field	Description
MAC address	MAC address of a multicast group.
VLAN ID	ID of the VLAN to which the network device identified by the MAC address belongs.
State	Status of the MAC address. If the multicast MAC address entry is static, this field displays Multicast .
Port/NickName	Outgoing ports or nickname of the Egress RB in a TRILL network for the packet that is sent to the MAC address in this MAC address entry. TRILL is not supported in the current software version.
Aging	Aging timer state. If this entry never expires, this field displays N .
1 mac address(es) found	One static multicast MAC address entry is found.

Related commands

`mac-address multicast`

dot1p-priority (IGMP-snooping view)

Use `dot1p-priority` to set the 802.1p priority for IGMP messages globally.

Use `undo dot1p-priority` to restore the default.

Syntax

```
dot1p-priority priority
```

```
undo dot1p-priority
```

Default

The global 802.1p priority is 6 for IGMP messages.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for IGMP messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You can set the 802.1p priority globally for all VLANs in IGMP-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

```
# Set the 802.1p priority for IGMP messages to 3 globally.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dot1p-priority 3
```

Related commands

igmp-snooping dot1p-priority

dscp

Use **dscp** to set the DSCP value for outgoing IGMP protocol packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value is 48 for outgoing IGMP protocol packets.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the ToS field of an IP packet to determine the transmission priority of the packet. A greater DSCP value represents a higher priority.

Examples

```
# Set the DSCP value to 63 for outgoing IGMP protocol packets.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dscp 63
```

enable (IGMP-snooping view)

Use **enable** to enable IGMP snooping for VLANs.

Use **undo enable** to disable IGMP snooping for VLANs.

Syntax

enable vlan *vlan-list*

undo enable vlan *vlan-list*

Default

IGMP snooping status in a VLAN is consistent with the global IGMP snooping status.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

You must enable the IGMP snooping feature by using the **igmp-snooping** command before you enable IGMP snooping for VLANs.

You can enable IGMP snooping for multiple VLANs by using this command in IGMP-snooping view or for a VLAN by using the **igmp-snooping enable** command in VLAN view. The configuration in IGMP-snooping view has the same priority as the configuration in VLAN view, and the most recent configuration takes effect.

Examples

Enable the IGMP snooping feature, and then enable IGMP snooping for VLAN 2 through VLAN 10.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] enable vlan 2 to 10
```

Related commands

igmp-snooping

igmp-snooping enable

entry-limit (IGMP-snooping view)

Use **entry-limit** to globally set the maximum number of IGMP snooping forwarding entries, including dynamic entries and static entries.

Use **undo entry-limit** to restore the default.

Syntax

```
entry-limit limit
```

```
undo entry-limit
```

Default

The maximum number of IGMP snooping forwarding entries is 4294967295.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of IGMP snooping forwarding entries, in the range of 0 to 4294967295.

Examples

```
# Set the global maximum number of IGMP snooping forwarding entries to 512.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] entry-limit 512
```

fast-leave (IGMP-snooping view)

Use **fast-leave** to enable fast-leave processing globally.

Use **undo fast-leave** to disable fast-leave processing globally.

Syntax

```
fast-leave [ vlan vlan-list ]
undo fast-leave [ vlan vlan-list ]
```

Default

Fast-leave processing is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for a multicast group when the port receives a leave message.

You can enable fast-leave processing globally for all ports in IGMP-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

```
# Globally enable fast-leave processing for VLAN 2.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] fast-leave vlan 2
```

Related commands

```
igmp-snooping fast-leave
```

global-enable (IGMP-snooping view)

Use **global-enable** to enable IGMP snooping globally.

Use **undo global-enable** to disable IGMP snooping globally.

Syntax

```
global-enable
```

```
undo global-enable
```

Default

IGMP snooping is disabled globally.

Views

IGMP-snooping view

Predefined user roles

network-admin

Usage guidelines

To configure other IGMP snooping features for VLANs, you must enable IGMP snooping for the specific VLANs even though IGMP snooping is enabled globally.

Examples

```
# Enable IGMP snooping globally.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] global-enable
```

Related commands

enable (IGMP-snooping view)

igmp-snooping

igmp-snooping disable

igmp-snooping enable

group-policy (IGMP-snooping view)

Use **group-policy** to globally configure a multicast group policy to control the multicast groups that hosts can join.

Use **undo group-policy** to globally delete multicast group policies.

Syntax

```
group-policy ipv4-acl-number [ vlan vlan-list ]
undo group-policy [ vlan vlan-list ]
```

Default

No multicast group policies exist. Hosts can join any multicast groups.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

A multicast group policy filters IGMP reports to control the multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send IGMP reports.

You can configure a multicast group policy globally for all ports in IGMP-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

To match the following IGMP reports, set the **source** *source-address source-wildcard* option to 0.0.0.0:

- IGMPv1 and IGMPv2 reports.
- IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs for all ports in different VLANs. If you configure multiple ACLs for all ports in the same VLAN, the most recent configuration takes effect.

Examples

```
# Configure a multicast group policy for VLAN 2 so that hosts in VLAN 2 can join only multicast group 225.1.1.1.
```

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] igmp-snooping
[Sysname-igmp-snooping] group-policy 2000 vlan 2
```

Related commands

```
igmp-snooping group-policy
```

host-aging-time (IGMP-snooping view)

Use **host-aging-time** to set the aging timer for dynamic member ports globally.

Use **undo host-aging-time** to restore the default.

Syntax

```
host-aging-time seconds
```

```
undo host-aging-time
```

Default

The aging timer for dynamic member ports is 260 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs in IGMP-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[IGMP general query interval] + [maximum response time for IGMP general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[IGMP general query interval] × 2 + [maximum response time for IGMP general queries]

Examples

```
# Set the global aging timer for dynamic member ports to 300 seconds.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] host-aging-time 300
```

Related commands

igmp-snooping host-aging-time

host-tracking (IGMP-snooping view)

Use **host-tracking** to enable host tracking globally.

Use **undo host-tracking** to disable host tracking globally.

Syntax

host-tracking

undo host-tracking

Default

Host tracking is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Usage guidelines

You can enable host tracking globally for all VLANs in IGMP-snooping view or for a VLAN in VLAN view. For a VLAN, the global configuration has the same priority as the VLAN-specific configuration.

Examples

```
# Enable host tracking globally.
<Sysname> system-view
[Sysname] igmp-snooping
```

```
[Sysname-igmp-snooping] host-tracking
```

Related commands

```
display igmp-snooping host-tracking
```

```
igmp-snooping host-tracking
```

igmp-snooping

Use `igmp-snooping` to enable the IGMP snooping feature and enter IGMP-snooping view.

Use `undo igmp-snooping` to disable the IGMP snooping feature.

Syntax

```
igmp-snooping
```

```
undo igmp-snooping
```

Default

The IGMP snooping feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If you disable the IGMP snooping feature, IGMP snooping is disabled in all VLANs.

Examples

```
# Enable the IGMP snooping feature and enter IGMP-snooping view.
```

```
<Sysname> system-view
```

```
[Sysname] igmp-snooping
```

```
[Sysname-igmp-snooping]
```

Related commands

```
enable (IGMP-snooping view)
```

```
igmp-snooping enable
```

```
igmp-snooping disable
```

igmp-snooping access-policy

Use `igmp-snooping access-policy` to configure an IGMP snooping access control policy.

Use `undo igmp-snooping access-policy` to delete an IGMP snooping access control policy.

Syntax

```
igmp-snooping access-policy ipv4-acl-number
```

```
undo igmp-snooping access-policy { ipv4-acl-number | all }
```

Default

No IGMP snooping access control policies exist. Multicast users can join or leave any multicast groups.

Views

User profile view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL by its number, in the range of 2000 to 3999. Multicast users can join or leave only the multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, multicast users cannot join or leave any multicast groups.

a11: Specifies all IGMP snooping access control policies.

Usage guidelines

You can repeat this command to configure multiple IGMP snooping access control policies. A multicast user can join or leave a multicast group if its IGMP report or leave message is permitted by one of the IGMP snooping access control policies.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

To match the following IGMP messages, set the **source** *source-address source-wildcard* option to 0.0.0.0:

- IGMPv1 report and leave messages.
 - IGMPv2 report and leave messages.
 - IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

Examples

In user profile **abc**, configure an IGMP snooping access control policy to allow multicast users to join or leave only multicast group 225.1.1.1.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 225.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] user-profile abc
[Sysname-user-profile-abc] igmp-snooping access-policy 2001
```

igmp-snooping dot1p-priority

Use **igmp-snooping dot1p-priority** to set the 802.1p priority for IGMP messages in a VLAN.

Use **undo igmp-snooping dot1p-priority** to restore the default.

Syntax

```
igmp-snooping dot1p-priority priority
```

```
undo igmp-snooping dot1p-priority
```

Default

The 802.1p priority is 6 for IGMP messages in a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for IGMP messages, in the range of 0 to 7. The greater the value, the higher the priority.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the 802.1p priority for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. The VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and set the 802.1p priority for IGMP messages to 3.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping dot1p-priority 3
```

Related commands

dot1p-priority (IGMP-snooping view)

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping drop-unknown

Use **igmp-snooping drop-unknown** to enable dropping unknown multicast data packets for a VLAN.

Use **undo igmp-snooping drop-unknown** to disable dropping unknown multicast data packets for a VLAN.

Syntax

igmp-snooping drop-unknown

undo igmp-snooping drop-unknown

Default

Dropping unknown multicast data packets is disabled. Unknown multicast data packets are flooded.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

```
# In VLAN 2, enable IGMP snooping, and enable dropping unknown multicast data packets.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping drop-unknown
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping { disable | enable }

Use **igmp-snooping enable** to enable IGMP snooping for a VLAN.

Use **igmp-snooping disable** to disable IGMP snooping for a VLAN.

Use **undo igmp-snooping** to restore the IGMP snooping status in a VLAN to the global IGMP snooping status.

Syntax

```
igmp-snooping { disable | enable }
```

```
undo igmp-snooping
```

Default

The IGMP snooping status in a VLAN is consistent with the global IGMP snooping status.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable the IGMP snooping feature by using the **igmp-snooping** command before you enable IGMP snooping for a VLAN.

You can enable IGMP snooping for a VLAN by using this command in VLAN view or for multiple VLANs by using the **enable** command in IGMP-snooping view. The configuration in VLAN view has the same priority as the configuration in IGMP-snooping view, and the most recent configuration takes effect.

Examples

```
# Enable the IGMP snooping feature, and then enable IGMP snooping for VLAN 2.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
```

```
# Disable IGMP snooping for VLAN 2.
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping disable
```

Related commands

enable (IGMP-snooping view)
igmp-snooping

igmp-snooping fast-leave

Use **igmp-snooping fast-leave** to enable fast-leave processing on a port.

Use **undo igmp-snooping fast-leave** to disable fast-leave processing on a port.

Syntax

```
igmp-snooping fast-leave [ vlan vlan-list ]
undo igmp-snooping fast-leave [ vlan vlan-list ]
```

Default

Fast-leave processing is disabled on a port.

Views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for a multicast group when the port receives a leave message.

You can enable fast-leave processing for a port in interface view or globally for all ports in IGMP-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

```
# Enable fast-leave processing for VLAN 2 on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping fast-leave vlan 2
```

Related commands

fast-leave (IGMP-snooping view)

igmp-snooping general-query source-ip

Use **igmp-snooping general-query source-ip** to configure the source IP address for IGMP general queries.

Use **undo igmp-snooping general-query source-ip** to restore the default.

Syntax

```
igmp-snooping general-query source-ip ip-address
```

```
undo igmp-snooping general-query source-ip
```

Default

In a VLAN, the source IP address of IGMP general queries is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP general queries.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

```
# In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP general queries.
```

```
<Sysname> system-view
```

```
[Sysname] igmp-snooping
```

```
[Sysname-igmp-snooping] quit
```

```
[Sysname] vlan 2
```

```
[Sysname-vlan2] igmp-snooping enable
```

```
[Sysname-vlan2] igmp-snooping general-query source-ip 10.1.1.1
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping group-limit

Use **igmp-snooping group-limit** to set the maximum number of multicast groups that a port can join.

Use **undo igmp-snooping group-limit** to remove the limit on the maximum number of multicast groups that a port can join.

Syntax

```
igmp-snooping group-limit limit [ vlan vlan-list ]
```

```
undo igmp-snooping group-limit [ vlan vlan-list ]
```

Default

No limit is placed on the maximum number of multicast groups that a port can join.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of multicast groups that a port can join, in the range of 0 to 4294967295.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id to end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

Examples

On GigabitEthernet 1/0/1, set the maximum number of multicast groups the port can join in VLAN 2 to 10.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-limit 10 vlan 2
```

igmp-snooping group-policy

Use **igmp-snooping group-policy** to configure a multicast group policy on a port to control the multicast groups that hosts attached to the port can join.

Use **undo igmp-snooping group-policy** to delete multicast group policies on a port.

Syntax

```
igmp-snooping group-policy ipv4-acl-number [ vlan vlan-list ]
undo igmp-snooping group-policy [ vlan vlan-list ]
```

Default

No multicast group policies exist on a port. Hosts attached to the port can join any multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv4-acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join multicast groups.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id to end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

A multicast group policy filters IGMP reports to control the multicast groups that hosts can join.

This command does not take effect on static member ports, because static member ports do not send IGMP reports.

You can configure a multicast group policy for a port in interface view or globally for all ports in IGMP-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv4 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-wildcard* option specifies a multicast group address.
- In an advanced ACL, the **source** *source-address source-wildcard* option specifies a multicast source address. The **destination** *dest-address dest-wildcard* option specifies a multicast group address.

To match the following IGMP reports, set the **source** *source-address source-wildcard* option to 0.0.0.0:

- IGMPv1 and IGMPv2 reports.
- IGMPv3 IS_EX and IGMPv3 TO_EX reports that do not carry multicast source addresses.
- Among the other optional parameters, only the **fragment** keyword and the **time-range** *time-range-name* option take effect.

You can configure different ACLs on a port for different VLANs. If you configure multiple ACLs on a port for the same VLAN, the most recent configuration takes effect.

Examples

On GigabitEthernet 1/0/1, configure a multicast group policy for VLAN 2 so that hosts in VLAN 2 can join only multicast group 225.1.1.1.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
```

Related commands

group-policy (IGMP-snooping view)

igmp-snooping host-aging-time

Use **igmp-snooping host-aging-time** to set the aging timer for dynamic member ports in a VLAN.

Use **undo igmp-snooping host-aging-time** to restore the default.

Syntax

igmp-snooping host-aging-time *seconds*

undo igmp-snooping host-aging-time

Default

The aging timer for dynamic member ports is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic member ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the timer for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

[IGMP general query interval] + [maximum response time for IGMP general queries]

As a best practice, set the aging timer of dynamic member ports to the value calculated by using the following formula:

[IGMP general query interval] × 2 + [maximum response time for IGMP general queries]

Examples

In VLAN 2, enable IGMP snooping, and set the aging timer for dynamic member ports to 300 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping host-aging-time 300
```

Related commands

enable (IGMP-snooping view)

host-aging-time (IGMP-snooping view)

igmp-snooping enable

igmp-snooping host-join

Use **igmp-snooping host-join** to configure a port as a simulated member host for a multicast group.

Use **undo igmp-snooping host-join** to remove the configuration of a simulated member host for a multicast group.

Syntax

```
igmp-snooping host-join group-address [ source-ip source-address ] vlan vlan-id
```

```
undo igmp-snooping host-join { group-address [ source-ip source-address ]  
vlan vlan-id | all }
```

Default

A port is not configured as a simulated member host for multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group in the range of 224.0.1.0 to 239.255.255.255.

source-ip *source-address*: Specifies a multicast source by its IP address. If you specify a multicast source, this command configures the port as a simulated member host for a multicast source and group. If you do not specify a multicast source, this command configures the port as a simulated member host for a multicast group. This option takes effect on IGMPv3 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all multicast groups.

Usage guidelines

The version of IGMP running on a simulated member host is the same as the version of IGMP snooping running on the port. The port ages out in the same way as a dynamic member port.

Examples

```
# Configure GigabitEthernet 1/0/1 as a simulated member host of the multicast source and group  
(1.1.1.1, 232.1.1.1) in VLAN 2.
```

```
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] quit  
[Sysname] vlan 2  
[Sysname-vlan2] igmp-snooping enable  
[Sysname-vlan2] igmp-snooping version 3  
[Sysname-vlan2] quit  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] igmp-snooping host-join 232.1.1.1 source-ip 1.1.1.1 vlan  
2
```

igmp-snooping host-tracking

Use **igmp-snooping host-tracking** to enable host tracking for a VLAN.

Use **undo igmp-snooping host-tracking** to disable host tracking for a VLAN.

Syntax

```
igmp-snooping host-tracking
```

```
undo igmp-snooping host-tracking
```

Default

Host tracking is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command for the VLAN.

You can enable host tracking for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration has the same priority as the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and then enable host tracking.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping host-tracking
```

Related commands

```
display igmp-snooping host-tracking
host-tracking (IGMP-snooping view)
igmp-snooping enable
```

igmp-snooping last-member-query-interval

Use `igmp-snooping last-member-query-interval` to set the IGMP last member query interval for a VLAN.

Use `undo igmp-snooping last-member-query-interval` to restore the default.

Syntax

```
igmp-snooping last-member-query-interval interval
undo igmp-snooping last-member-query-interval
```

Default

The IGMP last member query interval is 1 second.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP last member query interval in the range of 1 to 25 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the interval for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and set the IGMP last member query interval to 3 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping last-member-query-interval 3
```

Related commands

enable (IGMP-snooping view)
igmp-snooping enable
last-member-query-interval (IGMP-snooping view)

igmp-snooping leave source-ip

Use **igmp-snooping leave source-ip** to configure the source IP address for IGMP leave messages.

Use **undo igmp-snooping leave source-ip** to restore the default.

Syntax

```
igmp-snooping leave source-ip ip-address  
undo igmp-snooping leave source-ip
```

Default

In a VLAN, the source IP address of IGMP leave messages is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP leave messages.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP leave messages.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping leave source-ip 10.1.1.1
```

Related commands

enable (IGMP-snooping view)
igmp-snooping enable

igmp-snooping max-response-time

Use **igmp-snooping max-response-time** to set the maximum response time for IGMP general queries in a VLAN.

Use **undo igmp-snooping max-response-time** to restore the default.

Syntax

igmp-snooping max-response-time *seconds*
undo igmp-snooping max-response-time

Default

The maximum response time for IGMP general queries is 10 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for IGMP general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the time for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the maximum response time for IGMP general queries to be less than the IGMP general query interval.

Examples

In VLAN 2, enable IGMP snooping, and set the maximum response time for IGMP general queries to 5 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping max-response-time 5
```

Related commands

enable (IGMP-snooping view)
igmp-snooping enable
igmp-snooping query-interval
max-response-time (IGMP-snooping view)

igmp-snooping overflow-replace

Use **igmp-snooping overflow-replace** to enable multicast group replacement on a port.

Use **undo igmp-snooping overflow-replace** to disable multicast group replacement on a port.

Syntax

```
igmp-snooping overflow-replace [ vlan vlan-list ]  
undo igmp-snooping overflow-replace [ vlan vlan-list ]
```

Default

Multicast group replacement is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id to end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

You can enable multicast group replacement for a port in interface view or globally for all ports in IGMP-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

```
# On GigabitEthernet 1/0/1, enable multicast group replacement for VLAN 2.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] igmp-snooping overflow-replace vlan 2
```

Related commands

overflow-replace (IGMP-snooping view)

igmp-snooping proxy enable

Use **igmp-snooping proxy enable** to enable IGMP snooping proxying for a VLAN.

Use **undo igmp-snooping proxy enable** to disable IGMP snooping proxying for a VLAN.

Syntax

```
igmp-snooping proxy enable  
undo igmp-snooping proxy enable
```

Default

IGMP snooping proxying is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

This command does not take effect on a VLAN that is a sub-VLAN of a multicast VLAN.

Examples

```
# In VLAN 2, enable IGMP snooping, and enable IGMP snooping proxying.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping proxy enable
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

subvlan (multicast-VLAN view)

igmp-snooping querier

Use **igmp-snooping querier** to enable the IGMP snooping querier.

Use **undo igmp-snooping querier** to disable the IGMP snooping querier.

Syntax

```
igmp-snooping querier
undo igmp-snooping querier
```

Default

The IGMP snooping querier is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

For a sub-VLAN of a multicast VLAN, this command takes effect only after you remove the sub-VLAN from the multicast VLAN.

Examples

```
# In VLAN 2, enable IGMP snooping, and enable the IGMP snooping querier.
```

```
<Sysname> system-view
[Sysname] igmp-snooping
```

```
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping querier
```

Related commands

enable (IGMP-snooping view)
igmp-snooping enable
subvlan (multicast VLAN view)

igmp-snooping querier-election

Use **igmp-snooping querier-election** to enable IGMP snooping querier election for a VLAN.

Use **undo igmp-snooping querier-election** to disable IGMP snooping querier election for a VLAN.

Syntax

igmp-snooping querier-election
undo igmp-snooping querier-election

Default

IGMP snooping querier election is disabled for a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

For IGMP snooping querier election to take effect, you must enable the IGMP snooping querier.

Examples

In VLAN 2, enable IGMP snooping, and enable IGMP snooping querier election.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping querier
[Sysname-vlan2] igmp-snooping querier-election
```

Related commands

igmp-snooping querier

igmp-snooping query-interval

Use **igmp-snooping query-interval** to set the IGMP general query interval for a VLAN.

Use **undo igmp-snooping query-interval** to restore the default.

Syntax

```
igmp-snooping query-interval interval  
undo igmp-snooping query-interval
```

Default

The IGMP general query interval is 125 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP general query interval in the range of 2 to 31744 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

To avoid mistakenly deleting multicast group members, set the IGMP general query interval to be greater than the maximum response time for IGMP general queries.

Examples

In VLAN 2, enable IGMP snooping, and set the IGMP general query interval to 20 seconds.

```
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] quit  
[Sysname] vlan 2  
[Sysname-vlan2] igmp-snooping enable  
[Sysname-vlan2] igmp-snooping query-interval 20
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping max-response-time

igmp-snooping querier

max-response-time

igmp-snooping report source-ip

Use **igmp-snooping report source-ip** to configure the source IP address for IGMP reports.

Use **undo igmp-snooping report source-ip** to restore the default.

Syntax

```
igmp-snooping report source-ip ip-address  
undo igmp-snooping report source-ip
```

Default

In a VLAN, the source IP address of IGMP reports is the IP address of the current VLAN interface. If the current VLAN interface does not have an IP address, the source IP address is 0.0.0.0.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP reports.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP reports.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping report source-ip 10.1.1.1
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping router-aging-time

Use **igmp-snooping router-aging-time** to set the aging timer for dynamic router ports in a VLAN.

Use **undo igmp-snooping router-aging-time** to restore the default.

Syntax

igmp-snooping router-aging-time *seconds*

undo igmp-snooping router-aging-time

Default

The aging timer for dynamic router ports is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can set the timer for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

In VLAN 2, enable IGMP snooping, and set the aging timer for dynamic router ports to 100 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping router-aging-time 100
```

Related commands

enable (IGMP-snooping view)
igmp-snooping enable
router-aging-time (IGMP-snooping view)

igmp-snooping router-port-deny

Use **igmp-snooping router-port-deny** to disable a port from becoming a dynamic router port.

Use **undo igmp-snooping router-port-deny** to allow a port to become a dynamic router port.

Syntax

```
igmp-snooping router-port-deny [ vlan vlan-list ]
undo igmp-snooping router-port-deny [ vlan vlan-list ]
```

Default

A port is allowed to become a dynamic router port.

Views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you specify VLANs, this command takes effect only when the port belongs to the specified VLANs. If you do not specify a VLAN, this command takes effect on all VLANs to which the port belongs.

Examples

Disable GigabitEthernet 1/0/1 from becoming a dynamic router port in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping router-port-deny vlan 2
```

igmp-snooping source-deny

Use **igmp-snooping source-deny** to enable multicast source port filtering on a port to discard all multicast data packets.

Use **undo igmp-snooping source-deny** to disable multicast source port filtering on a port.

Syntax

```
igmp-snooping source-deny
undo igmp-snooping source-deny
```

Default

Multicast source port filtering is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

You can enable this feature for a port in interface view or for the specified ports in IGMP-snooping view. For a port, the configuration in interface view has the same priority as the configuration in IGMP-snooping view, and the most recent configuration takes effect.

Examples

```
# Enable source port filtering for multicast data on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping source-deny
```

Related commands

source-deny (IGMP-snooping view)

igmp-snooping special-query source-ip

Use **igmp-snooping special-query source-ip** to configure the source IP address for IGMP group-specific queries.

Use **undo igmp-snooping special-query source-ip** to restore the default.

Syntax

```
igmp-snooping special-query source-ip ip-address
undo igmp-snooping special-query source-ip
```

Default

In a VLAN, the source IP address of IGMP group-specific queries is one of the following:

- The source address of IGMP group-specific queries if the IGMP snooping querier of the VLAN has received IGMP general queries.
- The IP address of the current VLAN interface if the IGMP snooping querier does not receive an IGMP general query.
- 0.0.0.0 if the IGMP snooping querier does not receive an IGMP general query and the current VLAN interface does not have an IP address.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for IGMP group-specific queries.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

Examples

In VLAN 2, enable IGMP snooping, and specify 10.1.1.1 as the source IP address of IGMP group-specific queries.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping special-query source-ip 10.1.1.1
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping static-group

Use **igmp-snooping static-group** to configure a port as a static member port of a multicast group.

Use **undo igmp-snooping static-group** to remove the configuration of static member ports.

Syntax

```
igmp-snooping static-group group-address [ source-ip source-address ]
vlan vlan-id
```

```
undo igmp-snooping static-group { group-address [ source-ip
source-address ] vlan vlan-id | all }
```

Default

A port is not a static member port of a multicast group.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

source-ip *source-address*: Specifies a multicast source by its IP address. If you specify a multicast source, this command configures the port as a static member port for a multicast source and group. If you do not specify a multicast source, this command configures the port as a static member port for a multicast group. This option takes effect on IGMPv3 snooping devices.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

all: Specifies all multicast groups.

Examples

Configure GigabitEthernet 1/0/1 as a static member port of the multicast source and group (1.1.1.1, 225.0.0.1) in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-group 225.0.0.1 source-ip 1.1.1.1
vlan 2
```

igmp-snooping static-router-port

Use **igmp-snooping static-router-port** to configure a port as a static router port.

Use **undo igmp-snooping static-router-port** to remove the configuration of static router ports.

Syntax

```
igmp-snooping static-router-port vlan vlan-id
undo igmp-snooping static-router-port { all | vlan vlan-id }
```

Default

A port is not a static router port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

all: Specifies all VLANs.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

Examples

Configure GigabitEthernet 1/0/1 as a static router port in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-router-port vlan 2
```

igmp-snooping version

Use `igmp-snooping version` to specify an IGMP snooping version for a VLAN.

Use `undo igmp-snooping version` to restore the default.

Syntax

```
igmp-snooping version version-number  
undo igmp-snooping version
```

Default

The IGMP snooping version in a VLAN is 2.

Views

VLAN view

Predefined user roles

network-admin

Parameters

version-number: Specifies an IGMP snooping version, 2 or 3.

Usage guidelines

You must enable IGMP snooping for a VLAN before you execute this command.

You can specify the version for a VLAN in VLAN view or for the specified VLANs in IGMP-snooping view. The VLAN-specific configuration has the same priority as the configuration in IGMP-snooping view, and the most recent configuration takes effect.

Examples

In VLAN 2, enable IGMP snooping, and specify IGMP snooping version 3.

```
<Sysname> system-view  
[Sysname] igmp-snooping  
[Sysname-igmp-snooping] quit  
[Sysname] vlan 2  
[Sysname-vlan2] igmp-snooping enable  
[Sysname-vlan2] igmp-snooping version 3
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

version (IGMP-snooping view)

last-member-query-interval (IGMP-snooping view)

Use `last-member-query-interval` to set the IGMP last member query interval globally.

Use `undo last-member-query-interval` to restore the default.

Syntax

```
last-member-query-interval interval  
undo last-member-query-interval
```

Default

The IGMP last member query interval is 1 second.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

interval: Specifies an IGMP last member query interval in the range of 1 to 25 seconds.

Usage guidelines

You can set the interval for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

```
# Set the global IGMP last member query interval to 3 seconds.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] last-member-query-interval 3
```

Related commands

igmp-snooping last-member-query-interval

mac-address multicast

Use **mac-address multicast** to configure a static multicast MAC address entry.

Use **undo mac-address multicast** to delete a static multicast MAC address entry.

Syntax

In system view:

```
mac-address multicast mac-address interface interface-list vlan vlan-id
undo mac-address [ multicast ] [ [ mac-address [ interface interface-list ] ]
vlan vlan-id ]
```

In Layer 2 aggregate interface view or Layer 2 Ethernet interface view:

```
mac-address multicast mac-address vlan vlan-id
undo mac-address [ multicast ] mac-address vlan vlan-id
```

Default

No static multicast MAC address entries exist.

Views

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a static multicast MAC address, in the format of H-H-H. You must specify an unused multicast MAC address. A multicast MAC address is a MAC address in which the least significant bit of the most significant octet is 1.

interface *interface-list*: Specifies a space-separated list of up to four interface items. Each item specifies an interface or an interface list in the format of *start-interface-type interface-number to end-interface-type interface-number*. The *interface-type interface-number* argument specifies an interface by its type and number. The available interface types include Layer 2 Ethernet interfaces and Layer 2 aggregate interfaces.

vlan *vlan-id*: Specifies an existing VLAN by its VLAN ID in the range of 1 to 4094. The system gives a prompt if the specified interface does not belong to the VLAN.

Usage guidelines

You do not need to enable IP multicast routing before you execute this command.

You can configure static multicast MAC address entries for the specified interfaces in system view or for the current interface in interface view.

If you do not specify the **multicast** keyword in the **undo mac-address** command, all static unicast MAC address entries and static multicast MAC entries are deleted.

Examples

Configure a static multicast MAC address entry. In the entry, the multicast MAC address is 0100-5E00-0003 and the outgoing ports are GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 in VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address multicast 0100-5e00-0003 interface gigabitethernet 1/0/1 to
gigabitethernet 1/0/5 vlan 2
```

Configure a static multicast MAC address entry on GigabitEthernet 1/0/1. In the entry, the multicast MAC address is 0100-5E00-0003 and the outgoing port is GigabitEthernet 1/0/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address multicast 0100-5e00-0003 vlan 2
```

Related commands

```
display mac-address multicast
```

max-response-time (IGMP-snooping view)

Use **max-response-time** to set the maximum response time for IGMP general queries globally.

Use **undo max-response-time** to restore the default.

Syntax

```
max-response-time seconds
```

```
undo max-response-time
```

Default

The maximum response time for IGMP general queries is 10 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies the maximum response time for IGMP general queries, in the range of 1 to 3174 seconds.

Usage guidelines

You can set the time for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting multicast group members, set the maximum response time for IGMP general queries to be less than the IGMP general query interval.

Examples

```
# Set the global maximum response time for IGMP general queries to 5 seconds.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] max-response-time 5
```

Related commands

igmp-snooping max-response-time

igmp-snooping query-interval

overflow-replace (IGMP-snooping view)

Use **overflow-replace** to enable the multicast group replacement feature globally.

Use **undo overflow-replace** to disable the multicast group replacement feature globally.

Syntax

```
overflow-replace [ vlan vlan-list ]
undo overflow-replace [ vlan vlan-list ]
```

Default

The multicast group replacement feature is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The VLAN ID is in the range of 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This command takes effect only on the multicast groups that a port joins dynamically.

You can enable the multicast group replacement feature globally for all ports in IGMP-snooping view or for a port in interface view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

```
# Globally enable the multicast group replacement feature for VLAN 2.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] overflow-replace vlan 2
```

Related commands

```
igmp-snooping overflow-replace
```

report-aggregation (IGMP-snooping view)

Use **report-aggregation** to enable IGMP report suppression.

Use **undo report-aggregation** to disable IGMP report suppression.

Syntax

```
report-aggregation
undo report-aggregation
```

Default

IGMP report suppression is enabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Examples

```
# Disable IGMP report suppression.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] undo report-aggregation
```

reset igmp-snooping group

Use **reset igmp-snooping group** to clear information about dynamic IGMP snooping group entries.

Syntax

```
reset igmp-snooping group { group-address [ source-address ] | all } [ vlan vlan-id ]
```

Views

User view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

source-address: Specifies a multicast source address. If you do not specify a multicast source, this command clears information about dynamic IGMP snooping group entries for all multicast sources.

all: Specifies all multicast groups.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears information about dynamic IGMP snooping group entries for all VLANs.

Examples

```
# Clear information about all dynamic IGMP snooping group entries.
```

```
<Sysname> reset igmp-snooping group all
```

Related commands

```
display igmp-snooping group
```

reset igmp-snooping router-port

Use **reset igmp-snooping router-port** to clear dynamic router port information.

Syntax

```
reset igmp-snooping router-port { all | vlan vlan-id }
```

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all dynamic router ports.

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify a VLAN, this command clears dynamic router port information for all VLANs.

Examples

```
# Clear dynamic router port information.
```

```
<Sysname> reset igmp-snooping router-port all
```

Related commands

```
display igmp-snooping router-port
```

reset igmp-snooping statistics

Use **reset igmp-snooping statistics** to clear statistics for IGMP messages and PIMv2 hello messages learned through IGMP snooping.

Syntax

```
reset igmp-snooping statistics
```

Views

User view

Predefined user roles

network-admin

Examples

```
# Clear the statistics for all IGMP messages and PIMv2 hello messages learned through IGMP snooping.
```

```
<Sysname> reset igmp-snooping statistics
```

Related commands

```
display igmp-snooping statistics
```

reset l2-multicast fast-forwarding cache

Use **reset l2-multicast fast-forwarding cache** to clear Layer 2 multicast fast forwarding entries.

Syntax

```
reset l2-multicast fast-forwarding cache [ vlan vlan-id ]  
{ { source-address | group-address } * | all } [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears Layer 2 multicast fast forwarding entries for the master device.

all: Specifies all Layer 2 multicast fast forwarding entries.

Examples

```
# Clear all Layer 2 multicast fast forwarding entries.
```

```
<Sysname> reset l2-multicast fast-forwarding cache all
```

```
# Clear the Layer 2 multicast fast forwarding entry for the multicast source and group (20.0.0.2, 225.0.0.2).
```

```
<Sysname> reset l2-multicast fast-forwarding cache 20.0.0.2 225.0.0.2
```

Related commands

```
display l2-multicast fast-forwarding cache
```

router-aging-time (IGMP-snooping view)

Use **router-aging-time** to set the aging timer for dynamic router ports globally.

Use **undo router-aging-time** to restore the default.

Syntax

```
router-aging-time seconds
```

```
undo router-aging-time
```

Default

The aging timer for dynamic router ports is 260 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging timer for dynamic router ports, in the range of 1 to 8097894 seconds.

Usage guidelines

You can set the timer globally for all VLANs in IGMP-snooping view or for a VLAN in VLAN view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

```
# Set the global aging timer for dynamic router ports to 100 seconds.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] router-aging-time 100
```

Related commands

igmp-snooping router-aging-time

source-deny (IGMP-snooping view)

Use **source-deny** to enable multicast source port filtering on ports to discard all multicast data packets.

Use **undo source-deny** to disable multicast source port filtering on ports.

Syntax

```
source-deny port interface-list
undo source-deny port interface-list
```

Default

Multicast source port filtering is disabled.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

port *interface-list*: Specifies a space-separated list of port items. Each item specifies a port by its port type and number or a range of ports in the form of *start-interface-type interface-number to end-interface-type interface-number*.

Usage guidelines

You can enable this feature for the specified ports in IGMP-snooping view or for a port in interface view. For a port, the configuration in IGMP-snooping view has the same priority as the configuration in interface view, and the most recent configuration takes effect.

Examples

```
# Enable multicast source port filtering on ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Related commands

igmp-snooping source-deny

version (IGMP-snooping view)

Use **version** to specify an IGMP snooping version for VLANs.

Use **undo version** to restore the default.

Syntax

version *version-number* **vlan** *vlan-list*

undo version **vlan** *vlan-list*

Default

The IGMP snooping version in a VLAN is 2.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

version-number: Specifies an IGMP snooping version, 2 or 3.

vlan *vlan-list*: Specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN by its ID or a range of VLANs in the form of *start-vlan-id* to *end-vlan-id*. The VLAN ID is in the range of 1 to 4094.

Usage guidelines

You must enable IGMP snooping for the specified VLANs before you execute this command.

You can specify the version for the specified VLANs in IGMP-snooping view or for a VLAN in VLAN view. The configuration in IGMP-snooping view has the same priority as the VLAN-specific configuration, and the most recent configuration takes effect.

Examples

```
# Enable IGMP snooping for VLAN 2 through VLAN 10, and specify IGMP snooping version 3 for these VLANs.
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] enable vlan 2 to 10
[Sysname-igmp-snooping] version 3 vlan 2 to 10
```

Related commands

enable (IGMP-snooping view)

igmp-snooping enable

igmp-snooping version