Contents

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
 IGMP snooping: Enabled
 Drop-unknown: Disabled
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Report-aggregation: Enabled
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: Disabled
 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
Dot1p-priority: 2

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: Disabled
 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
 Dot1p-priority: --
```

Table 1 Command output

Field	Description
IGMP snooping	IGMP snooping status: • Enabled. • Disabled.
Drop-unknown	Status of dropping unknown multicast data: • 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: • Enabled. • Disabled.
Dot1p-priority	802.1p priority for IGMP messages. If the priority is not configured, this field displays two hyphens (--).
Querier	Whether the IGMP snooping querier is enabled.
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.

display igmp-snooping group

Use **display igmp-snooping group** to display dynamic IGMP snooping forwarding entries.

Syntax

display igmp-snooping 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 dynamic IGMP snooping forwarding 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 dynamic IGMP snooping 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 dynamic IGMP snooping forwarding entries for all VLANs.

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

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify this option, the command displays dynamic IGMP snooping forwarding entries on the master device.

Examples

Display detailed information about the dynamic IGMP snooping forwarding 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):
      XGE1/0/2        (00:03:23)
```

Table 2 Command output

Field	Description
Total 1 entries	Total number of dynamic IGMP snooping forwarding entries.
VLAN 2: Total 1 entries	Total number of dynamic IGMP snooping 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 any multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the specified device.

Field	Description
	• **slot**—The entry has a port that resides on a device other than the specified device.
FSM information	Finite state machine information of the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new and temporary entry. • **no info**—No entry exists.
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (1 in total)	Member ports, and the total number of the member ports.
(00:03:23)	Remaining aging time for the dynamic member port. • For a global port, this field is always displayed. • For a non-global port, this field is displayed if the port is on the master device. Otherwise, you must specify the **slot** *slot-number* option to display this field.

Related commands

> **reset igmp-snooping group**

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

Examples

> # Display dynamic router port information for VLAN 2.

```
<Sysname> display igmp-snooping router-port vlan 2
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    XGE1/0/1                 (00:01:30)
    XGE1/0/2                 (00:00:23)
```

Table 3 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs of the member devices that have router ports and the total number of the member devices (excluding the specified member device).
Router ports (2 in total)	Dynamic router ports, and the total number of the 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 non-global port, this field is displayed if the port is on the master device. Otherwise, you must specify the **slot** *slot-number* option to display this field.

Related commands

reset igmp-snooping router-port

display igmp-snooping static-group

Use **display igmp-snooping static**-**group** to display static IGMP snooping forwarding 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 static IGMP snooping forwarding 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 static IGMP snooping 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 static IGMP snooping forwarding entries for all VLANs.

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

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify this option, the command displays static IGMP snooping forwarding entries on the master device.

Examples

Display detailed information about the static IGMP snooping forwarding 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):
        XGE1/0/2
```

Table 4 Command output

Field	Description
Total 1 entries	Total number of static IGMP snooping forwarding entries.
VLAN 2: Total 1 entries	Total number of static IGMP snooping 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 any multicast sources.
Attribute	Entry attribute: • **global port**—The entry has a global port. • **local port**—The entry has a port that resides on the specified device. • **slot**—The entry has a port that resides on a device other than the specified device.
FSM information	Finite state machine information of the entry: • **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 of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (1 in total)	Member ports, and the total number of the 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*] [**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.

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

Examples

Display static router port information for VLAN 2.

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

```
XGE1/0/1
XGE1/0/2
```

Table 5 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs of the member devices that have router ports and the total number of the member devices (excluding the specified member device).
Router ports (2 in total)	Static router ports, and the total number of the 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 6 Command output

Field	Description
general queries	Number of IGMP general queries.
specific queries	Number of IGMP group-specific queries.

Field	Description
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 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 this option, the command displays information about the Layer 2 IP multicast groups on the master device.

Examples

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

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

VLAN 2: Total 1 IP entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: static, success
    Host slots (0 in total):
    Host ports (1 in total):
      XGE1/0/1                (S, SUC)
```

Table 7 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IP multicast groups.
VLAN 2: Total 1 IP 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 any multicast sources.
Attribute	Entry attribute: • **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 succeeds. • **fail**—Processing fails.
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (1 in total)	Member ports, and the total number of the member ports.
(S, SUC)	Port attribute: • **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 succeeds. • **F**—Processing fails. • **BC**—Broadcast port. The TRILL port floods the multicast traffic after the topology changes.

display l2-multicast ip forwarding

Use **display l2-multicast ip forwarding** to display Layer 2 IP multicast group 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 IP multicast group 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 IP multicast 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 Layer 2 IP multicast group entries for all VLANs.

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

Examples

Display Layer 2 IP multicast group entries for VLAN 2.

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

VLAN 2: Total 1 IP entries.
  (0.0.0.0, 224.1.1.1)
    Host slots (0 in total):
    Host ports (3 in total):
       XGE1/0/1
       XGE1/0/2
       XGE1/0/3
```

Table 8 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IP multicast group entries.
VLAN 2: Total 1 IP entries	Total number of Layer 2 IP multicast 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 any multicast sources.
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (3 in total)	Member ports, and the total number of the 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 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 this option, the command displays information about the Layer 2 MAC multicast groups on the master device.

Examples

Display information about the Layer 2 MAC multicast groups for VLAN 2.

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

VLAN 2: Total 1 MAC entries.
  MAC group address: 0100-5e01-0101
    Attribute: success
    Host slots (0 in total):
    Host ports (1 in total):
      XGE1/0/1
```

Table 9 Command output

Field	Description
Total 1 MAC entries	Total number of Layer 2 MAC multicast groups.
VLAN 2: Total 1 MAC entries	Total number of Layer 2 MAC multicast groups in VLAN 2.
Attribute	Entry attribute: • **success**—Processing succeeds. • **fail**—Processing fails.
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (1 in total)	Member ports, and the total number of the member ports.

display l2-multicast mac forwarding

Use **display l2-multicast mac forwarding** to display Layer 2 MAC multicast group 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 MAC multicast group 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 MAC multicast group entries for all VLANs.

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

Examples

Display Layer 2 MAC multicast group entries for VLAN 2.

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

```
Total 1 MAC entries.


VLAN 2: Total 1 MAC entries.
  MAC group address: 0100-5e01-0101
    Host slots (0 in total):
    Host ports (3 in total):
      XGE1/0/1
      XGE1/0/2
      XGE1/0/3
```

Table 10 Command output

Field	Description
Total 1 MAC entries	Total number of Layer 2 MAC multicast group entries.
VLAN 2: Total 1 MAC entries	Total number of Layer 2 MAC multicast group entries in VLAN 2.
MAC group address	Address of the MAC multicast group.
Host slots (0 in total)	Member IDs of the member devices that have member ports and the total number of the member devices (excluding the specified member device).
Host ports (3 in total)	Member ports, and the total number of the member ports.

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-number*

undo dot1p-priority

Default

The 802.1p priority for IGMP messages is not configured.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

priority-number: Specifies an 802.1p priority for IGMP messages, in the range of 0 to 7. A higher value means a higher 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

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 is disabled in a VLAN.

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 value range for the VLAN ID is 1 to 4094.

Usage guidelines

  You must enable IGMP snooping globally before you enable IGMP snooping for VLANs.

  You can enable IGMP snooping for the specified VLANs in IGMP-snooping view or for a VLAN in VLAN view. For a VLAN, 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 IGMP snooping globally, and 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 set the global 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 setting is 4294967295.

Views

> IGMP-snooping view

Predefined user roles

> network-admin

Parameters

> *limit*: Specifies the global 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 value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

> This feature enables the switch 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

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

group-policy (IGMP-snooping view)

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

Use **undo group-policy** to remove the configured global multicast group policy.

Syntax

group-policy *acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

Default

Global multicast group policies are not configured, and receiver hosts can join any multicast groups.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Receiver hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or the ACL does not contain valid rules, receiver 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 value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.

- 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:

  o IGMPv1 and IGMPv2 reports.

  o 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 ACL rules on a port in different VLANs. However, for a given VLAN, a newly configured ACL rule overrides the existing one.

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

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.

Examples

Globally configure a multicast group policy for VLAN 2 so that the hosts in this VLAN can join only multicast group 225.1.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-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 *interval*

undo host-aging-time

Default

The default setting is 260 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

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

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 aging timer for dynamic member ports to 300 seconds globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] host-aging-time 300
```

Related commands

igmp-snooping host-aging-time

igmp-snooping

Use **igmp-snooping** to enable IGMP snooping globally and enter IGMP-snooping view.

Use **undo igmp-snooping** to disable IGMP snooping globally.

Syntax

igmp-snooping

undo igmp-snooping

Default

IGMP snooping is globally disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable IGMP snooping globally 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 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-number*

undo igmp-snooping dot1p-priority

Default

The 802.1p priority for IGMP messages is not configured.

Views

VLAN view

Predefined user roles

network-admin

Parameters

priority-number: Specifies an 802.1p priority for IGMP messages, in the range of 0 to 7. A higher value means a higher 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. For a VLAN, 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 for a VLAN.

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

Syntax

igmp-snooping drop-unknown

undo igmp-snooping drop-unknown

Default

Dropping unknown multicast data in a VLAN is disabled, and unknown multicast data is flooded in the 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 the VLAN.

Examples

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

```
<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 enable

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

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

Syntax

igmp-snooping enable

undo igmp-snooping enable

Default

IGMP snooping is disabled in a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable IGMP snooping globally before you enable IGMP snooping for a VLAN.

You can enable IGMP snooping for a VLAN in VLAN view or for the specified VLANs in IGMP-snooping view. For a VLAN, 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 IGMP snooping globally and for VLAN 2.

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

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 value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

This feature enables the switch 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 Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-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

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 an IP address.

Usage guidelines

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

Examples

In VLAN 2, enable IGMP snooping, and configure 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 restore the default.

Syntax

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

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

Default

The default setting is 4294967295.

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 value range for the VLAN ID is 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

Set the maximum number of multicast groups that Ten-GigabitEthernet 1/0/1 in VLAN 2 can join to 10.
```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-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 the receiver hosts attached to the port can join.

Use **undo igmp-snooping group-policy** to remove the multicast group policy on a port.

Syntax

igmp-snooping group-policy *acl-number* [**vlan** *vlan-list*]

undo igmp-snooping group-policy [**vlan** *vlan-list*]

Default

Multicast group policies are not configured on a port, and the 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

acl-number: Specifies an IPv4 basic or advanced ACL by its number in the range of 2000 to 3999. Receiver hosts can join only the multicast groups that the ACL permits. If the ACL does not exist or the ACL does not contain valid rules, receiver 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 value range for the VLAN ID is 1 to 4094. If you do not specify a VLAN, this command takes effect on all VLANs.

Usage guidelines

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

- For the rule to take effect, do not specify the **vpn-instance** *vpn-instance* option.
- 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:

  o IGMPv1 and IGMPv2 reports.
  o 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 ACL rules on a port in different VLANs. However, for a given VLAN, a newly configured ACL rule overrides the existing one.

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.

Examples

Configure a multicast group policy for VLAN 2 on Ten-GigabitEthernet 1/0/1 so that hosts attached to the port in VLAN 2 can join only multicast group 225.1.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-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 the dynamic member ports in a VLAN.

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

Syntax

> **igmp-snooping host-aging-time** *interval*
>
> **undo igmp-snooping host-aging-time**

Default

The default setting is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

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

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]

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 the 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 simulated joining configuration.

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 Ten-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 ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] igmp-snooping host-join 232.1.1.1 source-ip 1.1.1.1
vlan 2
```

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 default setting 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

> The IGMP last member query interval determines the interval for sending IGMP group-specific queries and the maximum response time for IGMP group-specific queries in a VLAN.
>
> You must enable IGMP snooping for a VLAN before you execute this command for the VLAN.
>
> 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 a 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

> 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 a 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 configure 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 *interval*

undo igmp-snooping max-response-time

Default

The default setting is 10 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interval: 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 for the VLAN.

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

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.

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**
- **max-response-time** (IGMP-snooping view)

igmp-snooping overflow-replace

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

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

Syntax

igmp-snooping overflow-replace [**vlan** *vlan-list*]

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

Default

The multicast group replacement feature 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 value range for the VLAN ID is 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

Enable the multicast group replacement feature for VLAN 2 on Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] igmp-snooping overflow-replace vlan 2
```

Related commands

overflow-replace (IGMP-snooping 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.

This command takes effect on a sub-VLAN 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 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 in a VLAN 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 a 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

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 a 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 configure 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 the dynamic router ports in a VLAN.

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

Syntax

igmp-snooping router-aging-time *interval*

undo igmp-snooping router-aging-time

Default

The default setting is 260 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

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

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 the 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 restore the default.

Syntax

igmp-snooping router-port-deny [**vlan** *vlan-list*]

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

Default

A port can 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 Ten-GigabitEthernet 1/0/1 from becoming a dynamic router port in VLAN 2.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-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 the received 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, and the port can connect to both multicast sources and multicast receivers.

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 Ten-GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-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 a 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

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 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 a 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 configure 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 group member of a multicast group.

Use **undo igmp-snooping static-group** to remove a static group member.

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 group member of 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 by its IP 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 group member for a multicast source and group. If you do not specify a multicast source, this command configures the port as a static group member 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 VLANs.

Examples

Configure Ten-GigabitEthernet 1/0/1 as a static group member 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 ten-gigabitethernet 1/0/1
```

```
[Sysname-Ten-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 a static router port.

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

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

igmp-snooping version

Use **igmp-snooping version** to specify an IGMP snooping version.

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 for the VLAN.

You can specify the version for a VLAN in VLAN view or for the specified VLANs in IGMP-snooping view. For a VLAN, the configuration in VLAN view 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 global IGMP last member query interval.

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

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

Default

The global IGMP last member query 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

The IGMP last member query interval determines the interval for sending IGMP group-specific queries and the maximum response time for IGMP group-specific queries.

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 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

max-response-time (IGMP-snooping view)

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

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

Syntax

    max-response-time *interval*

    undo max-response-time

Default

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

Views

    IGMP-snooping view

Predefined user roles

    network-admin

Parameters

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

Usage guidelines

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

    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.

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

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 globally.

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 value range for the VLAN ID is 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

Enable the multicast group replacement feature globally 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 remove the dynamic IGMP snooping forwarding entries for multicast groups.

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 by its IP address in the range of 224.0.1.0 to 239.255.255.255.

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command removes the dynamic IGMP snooping forwarding 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 removes dynamic IGMP snooping forwarding entries for all VLANs.

Examples

Remove the dynamic IGMP snooping forwarding entries for all multicast groups.

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

Related commands

display igmp-snooping group

reset igmp-snooping router-port

Use **reset igmp-snooping router-port** to remove dynamic router ports.

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 removes dynamic router ports for all VLANs.

Examples

Remove all dynamic router ports.

```
<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 the 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

router-aging-time (IGMP-snooping view)

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

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

Syntax

router-aging-time *interval*

undo router-aging-time

Default

The global aging timer for dynamic router ports is 260 seconds.

Views

IGMP-snooping view

Predefined user roles

network-admin

Parameters

interval: 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 the received 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, and the ports can connect to both multicast sources and multicast receivers.

Views

> IGMP-snooping view

Predefined user roles

> network-admin

Parameters

> **port** *interface-list*: Specifies a port 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 Ten-GigabitEthernet 1/0/1 through Ten-GigabitEthernet 1/0/4.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] source-deny port ten-gigabitethernet 1/0/1 to
ten-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 default setting 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 value range for the VLAN ID is 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. For a VLAN, 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 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**