HPE FlexNetwork 5130 HI Switch Series

IP Multicast

Command Reference

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

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
 Global-enable: Enabled
 Drop-unknown: Disabled
 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: 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
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: 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
 Host-tracking: Disabled
 Dot1p-priority: --
 Proxy: Disabled
```

Table 1 Command output

Field	Description
Global-enable	Global IGMP snooping status: • Enabled. • Disabled.
IGMP snooping	IGMP snooping status in a VLAN: • **Enabled**. • **Disabled**. • **Globally enabled**. • **Inactive**—IGMP snooping configuration does not take effect.
Drop-unknown	Status of dropping unknown multicast data: • Enabled. • Disabled. • Globally enabled.
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.

Field	Description
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: • 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: • Enabled • Disabled. • Globally enabled.
Proxy	Status of IGMP snooping proxying: • 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*] [**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.

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.

3

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 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: • **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: • **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)	Remaining aging time for the dynamic member port. For a global port (such as Layer 2 aggregate interfaces), this field is always displayed. For a non-global port, this field is displayed when one of the following conditions exists: • 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

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: • 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.

Field	Description
Attribute	Entry attribute: • **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: • **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.

Field	Description
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: • **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: • **0x1**—The port is added to the entry because of packets passed through between cards. • **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: • **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):
      GE1/0/1                           (S, SUC)
```

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: • **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: • **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: • **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
                                            GE1/0/2
```

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 for the packet that is sent to the MAC address in this MAC address entry.
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 802.1p priority for IGMP messages is not configured. For IGMP messages created by the device, the 802.1p priority is 0. For IGMP messages to be forwarded, the device does not change the 802.1p priority.

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

drop-unknown (IGMP-snooping view)

Use **drop-unknown** to enable dropping unknown multicast data packets globally.

Use **undo drop-unknown** to disable dropping unknown multicast data packets globally.

Syntax

drop-unknown

undo drop-unknown

Default

Dropping unknown multicast data packets is disabled, and unknown multicast data packets are flooded.

Views

IGMP-snooping view

Predefined user roles

network-admin

Usage guidelines

You can enable this feature globally for all VLANs in IGMP-snooping view or for a VLAN in VLAN view.

The **igmp-snooping drop-unknown** command and the **drop-unknown** command in IGMP-snooping view are mutually exclusive. You cannot configure them on the same device.

Examples

\# Enable dropping unknown multicast data packets globally.

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

Related commands

igmp-snooping drop-unknown

enable (IGMP-snooping view)

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

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

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.

Views

> IGMP-snooping view

Predefined user roles

> network-admin

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:

  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 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 globally.

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 disable

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

Syntax

igmp-snooping disable

Default

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

Views

VLAN view

Predefined user roles

network-admin

Examples

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 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*

undo igmp-snooping dot1p-priority

Default

The 802.1p priority for IGMP messages is not configured. For IGMP messages created by the device, the 802.1p priority is 0. For IGMP messages to be forwarded, the device does not change the 802.1p priority.

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. 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 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.

You can enable this feature for a VLAN in VLAN view or globally for all VLANs in IGMP-snooping view.

The **igmp-snooping drop-unknown** command and the **drop-unknown** command in IGMP-snooping view are mutually exclusive. You cannot configure them on the same device.

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

    drop-unknown (IGMP-snooping view)

    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** to restore the IGMP snooping status in a VLAN to the global IGMP snooping status.

Syntax

igmp-snooping 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
```

Related commands

enable (IGMP-snooping view)

igmp-snooping

igmp-snooping disable

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 polices 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:

  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 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.

33

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 in a VLAN.

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 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 for a VLAN.

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 in a VLAN.

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.

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. 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 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 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 0100-0001-0001 and the outgoing ports are GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 in VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address multicast 0100-0001-0001 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 0100-0001-0001 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 0100-0001-0001 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. 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

igmp-snooping version

PIM snooping commands

display pim-snooping neighbor

Use **display pim-snooping neighbor** to display PIM snooping neighbor information.

Syntax

display pim-snooping neighbor [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

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. If you do not specify a VLAN, this command displays PIM snooping neighbor 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 PIM snooping neighbor information for the master device.

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

Examples

Display detailed information about PIM snooping neighbors for VLAN 2.

```
<Sysname> display pim-snooping neighbor vlan 2 verbose
Total 2 neighbors.

VLAN 2: Total 2 neighbors.
  10.1.1.2
    Slots (0 in total):
    Ports (1 in total):
      GE1/0/1                            (02:02:23)    LAN Prune Delay(T)
  10.1.1.3
    Slots (0 in total):
    Ports (1 in total):
      GE1/0/2                            (02:02:25)
```

Table 14 Command output

Field	Description
Total 2 neighbors	Total number of PIM snooping neighbors.
VLAN 2: Total 2 neighbors	Total number of PIM snooping neighbors in VLAN 2.
10.1.1.2	IP address of the PIM snooping neighbor.
Slots (0 in total)	Member IDs and total number of the member devices that have the neighbor, except for the specified member device or the master device when no member device is specified.
Ports (1 in total)	Ports where the PIM snooping neighbors reside, and the total number of

Field	Description
	the ports.
(02:02:23)	Remaining aging timer for a PIM snooping neighbor on the port. This field is always displayed for a global port (such as Layer 2 aggregate interfaces). For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
LAN Prune Delay	The PIM hello message sent by the PIM snooping neighbor has the LAN_Prune_Delay option.
(T)	The join message suppression feature has been disabled for the PIM snooping neighbor.

display pim-snooping router-port

Use **display pim-snooping router-port** to display PIM snooping router port information.

Syntax

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

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. If you do not specify a VLAN, this command displays PIM snooping router port information for all VLANs.

verbose: Displays detailed information about PIM snooping router ports. If you do not specify this keyword, the command displays brief information about PIM snooping 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 PIM snooping router port information for the master device.

Examples

Display brief information about PIM snooping router ports for VLAN 2.

```
<Sysname> display pim-snooping router-port vlan 2
VLAN 2:
  Router ports (2 in total):
    GE1/0/1                              (00:01:30)
    GE1/0/2                              (00:01:32)
```

Table 15 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs and total number of the member devices that have router ports, except for the specified member device or the master device when

Field	Description
	no member device is specified.
Router ports (2 in total)	Router ports and total number of router ports.
(00:01:30)	Remaining aging time for the router port. For a global port, this field is always displayed. For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

display pim-snooping routing-table

Use **display pim-snooping routing-table** to display PIM snooping routing entries.

Syntax

display pim-snooping routing-table [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

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. If you do not specify a VLAN, this command displays PIM snooping routing 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 PIM snooping routing entries for the master device.

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

Examples

Display detailed information about PIM snooping routing entries for VLAN 2.

```
<Sysname> display pim-snooping routing-table vlan 2 verbose
Total 1 entries.
FSM Flag: NI-no info, J-join, PP-prune pending

VLAN 2: Total 1 entries.
  (172.10.10.1, 225.1.1.1)
    FSM information: dummy
    Upstream neighbor: 20.1.1.1
      Upstream Slots (0 in total):
      Upstream Ports (1 in total):
        GE1/0/1
      Downstream Slots (0 in total):
      Downstream Ports (2 in total):
        GE1/0/2
```

```
          Expires: 00:03:01, FSM: J
       Downstream Neighbors (2 in total):
          7.1.1.1
            Expires: 00:59:19, FSM: J
          7.1.1.11
            Expires: 00:59:20, FSM: J
      GE1/0/3
        Expires: 00:02:21, FSM: PP
```

Table 16 Command output

Field	Description
Total 1 entries	Total number of (S, G) entries and (*, G) entries.
FSM Flag: NI-no info, J-join, PP-prune pending	State machine flag of the downstream port: • **NI**—Initial state. • **J**—Join. • **PP**—Prune pending.
VLAN 2: Total 1 entries	Total number of (S, G) entries and (*, G) entries in VLAN 2.
(172.10.10.1, 225.1.1.1)	(S, G) entry.
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**—The entry does not exist.
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry.
Upstream Slots (0 in total)	Member IDs and total number of the member devices that have the upstream neighbor, except for the specified member device or the master device when no member device is specified.
Upstream Ports (1 in total)	Upstream ports, and the total number of upstream ports. This field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
Downstream Slots (0 in total)	Member IDs and total number of the member devices that have downstream ports, except for the specified member device or the master device when no member device is specified.
Downstream Ports (2 in total)	Downstream ports of the upstream neighbor, and the total number of the downstream ports.
Downstream Neighbors (2 in total)	Downstream neighbors of the downstream port, and the total number of the downstream neighbors.
Expires: 00:03:01, FSM: J	Remaining aging time for the downstream port or downstream neighbor, and the finite state machine information. For a global port, this field is always displayed. For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

display pim-snooping statistics

Use **display pim-snooping statistics** to display statistics for the PIM messages learned through PIM snooping.

Syntax

display pim-snooping statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

\# Display statistics for the PIM messages learned through PIM snooping.

```
<Sysname> display pim-snooping statistics
Received PIMv2 hello:  100
Received PIMv2 join/prune:  100
Received PIMv2 error:  0
Received PIMv2 messages in total:  200
Received PIMv1 messages in total:  0
```

Table 17 Command output

Field	Description
Received PIMv2 hello	Number of received PIMv2 hello messages.
Received PIMv2 join/prune	Number of received PIMv2 join/prune messages.
Received PIMv2 error	Number of received PIMv2 messages with errors.
Received PIMv2 messages in total	Total number of received PIMv2 messages.
Received PIMv1 messages in total	Total number of received PIMv1 messages.

Related commands

reset pim-snooping statistics

pim-snooping enable

Use **pim-snooping enable** to enable PIM snooping for a VLAN.

Use **undo pim-snooping enable** to disable PIM snooping for a VLAN.

Syntax

pim-snooping enable

undo pim-snooping enable

Default

PIM snooping is disabled for a VLAN.

Views

VLAN view

network-admin

Usage guidelines

You must enable the IGMP snooping feature and enable IGMP snooping for a VLAN before you enable PIM snooping for the VLAN.

PIM snooping does not take effect on sub-VLANs of a multicast VLAN.

Examples

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

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

Related commands

igmp-snooping

igmp-snooping enable

pim-snooping graceful-restart join-aging-time

Use **pim-snooping graceful-restart join-aging-time** to set the aging time for global downstream ports and global router ports on the new master device after a master/subordinate switchover.

Use **undo pim-snooping graceful-restart join-aging-time** to restore the default.

Syntax

pim-snooping graceful-restart join-aging-time *seconds*

undo pim-snooping graceful-restart join-aging-time

Default

The default setting is 210 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging time in the range of 210 to 18000 seconds.

Usage guidelines

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

Global ports include Layer 2 aggregate interfaces. A global downstream port or a global router port is a global port that acts as a downstream port or router port, respectively.

Examples

In VLAN 2, set the aging time to 600 seconds for global downstream ports and global router ports on the new master device after a master/subordinate switchover.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] pim-snooping enable
[Sysname-vlan2] pim-snooping graceful-restart join-aging-time 600
```

Related commands

pim-snooping enable

pim-snooping graceful-restart neighbor-aging-time

Use **pim-snooping graceful-restart neighbor-aging-time** to set the aging time for global neighbor ports on the new master device after a master/subordinate switchover.

Use **undo pim-snooping graceful-restart neighbor-aging-time** to restore the default.

Syntax

pim-snooping graceful-restart neighbor-aging-time *seconds*

undo pim-snooping graceful-restart neighbor-aging-time

Default

The default setting is 105 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging time in the range of 105 to 18000 seconds.

Usage guidelines

You must enable PIM snooping in a VLAN before you execute this command.

Global ports include Layer 2 aggregate interfaces. A global neighbor port is a global port that acts as a neighbor port.

Examples

In VLAN 2, set the aging time to 300 seconds for global neighbor ports on the new master device after a master/subordinate switchover.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] pim-snooping enable
[Sysname-vlan2] pim-snooping graceful-restart neighbor-aging-time 300
```

Related commands

pim-snooping enable

reset pim-snooping statistics

Use **reset pim-snooping statistics** to clear statistics for the PIM messages learned through PIM snooping.

Syntax

reset pim-snooping statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear statistics for the PIM messages learned through PIM snooping.

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

Related commands

display pim-snooping statistics

Multicast VLAN commands

display multicast-vlan

Use **display multicast-vlan** to display information about multicast VLANs.

Syntax

display multicast-vlan [*vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id: Specifies a multicast VLAN ID in the range of 1 to 4094. If you do not specify a multicast VLAN ID, this command displays information about all multicast VLANs.

Examples

Display information about all multicast VLANs.

```
<Sysname> display multicast-vlan
Total 2 multicast VLANs.

Multicast VLAN 100:
  Sub-VLAN list(3 in total):
    2-3, 6
  Port list(3 in total):
    GE1/0/1
    GE1/0/2
    GE1/0/3

Multicast VLAN 200:
  Sub-VLAN list(0 in total):
  Port list(0 in total):
```

Table 18 Command output

Field	Description
Total 2 multicast VLANs	Total number of multicast VLANs.
Sub-VLAN list(3 in total)	Sub-VLAN list of the multicast VLAN, and the total number of the sub-VLANs.
Port list(3 in total)	Port list of the multicast VLAN, and the total number of the ports.

display multicast-vlan forwarding-table

Use **display multicast-vlan forwarding-table** to display multicast VLAN forwarding entries.

Syntax

display multicast-vlan forwarding-table [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *

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 224.0.0.0 to 239.255.255.255. If you do not specify a multicast group, this command displays multicast VLAN forwarding entries for all multicast groups.

mask { *mask-length* | *mask* }: Specifies a mask length or subnet mask for the multicast group address. The value range for the *mask-length* argument is 4 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

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

mask { *mask-length* | *mask* }: Specifies a mask length or subnet mask for the multicast source address. The value range for the *mask-length* argument is 0 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

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

subvlan *vlan-id*: Specifies a sub-VLAN by its VLAN ID. If you do not specify a sub-VLAN, this command displays multicast VLAN forwarding entries for all sub-VLANs.

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

Examples

Display all multicast VLAN forwarding entries.

```
<Sysname> display multicast-vlan forwarding-table
Multicast VLAN 100 Forwarding Table
Total 1 entries, 1 matched

00001. (1.1.1.1, 225.0.0.1)
    Flags: 0x10000
    Multicast VLAN: 100
    List of sub-VLANs (3 in total):
      1: VLAN 10
      2: VLAN 20
      3: VLAN 30
```

Table 19 Command output

Field	Description
Multicast VLAN 100 Forwarding Table	Forwarding entries for multicast VLAN 100.
Total 1 entries, 1 matched	Total number of (S, G) entries, and the number of matching entries.
00001	Sequence number of the (S, G) entry.

Field	Description
(1.1.1.1, 255.0.0.1)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. In this example, the value 0x10000 means that the entry has only one flag 0x10000. The following flags are available for an entry: • **0x1**—The entry is in inactive state. • **0x4**—The entry fails to update. • **0x8**—The sub-VLAN information fails to update for the entry. • **0x200**—The entry is in GR state. • **0x10000**—The entry is a multicast VLAN forwarding entry.
List of sub-VLANs (3 in total)	Sub-VLAN list of the multicast VLAN, and the total number of the sub-VLANs.

display multicast-vlan group

Use **display multicast-vlan group** to display information about multicast groups in multicast VLANs.

Syntax

display multicast-vlan group [*source-address* | *group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

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 for all multicast groups in multicast 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 multicast groups in multicast VLANs for the master device.

verbose: Displays detailed information.

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

Examples

Display detailed information about all multicast groups in multicast VLANs.

```
<Sysname> display multicast-vlan group verbose
Total 6 entries.
```

```
Multicast VLAN 10: Total 3 entries.
  (2.2.2.2, 225.1.1.2)
    Flags: 0x70000020
    Sub-VLANs (1 in total):
      VLAN 40
  (111.112.113.115, 225.1.1.4)
    Flags: 0x70000030
    Sub-VLANs (1 in total):
      VLAN 40
  (0.0.0.0, 226.1.1.6)
    Flags: 0x60000020
    Sub-VLANs (1 in total):
      VLAN 40

Multicast VLAN 20: Total 3 entries.
  (2.2.2.2, 225.1.1.2)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (111.112.113.115, 225.1.1.4)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (0.0.0.0, 226.1.1.6)
    Flags: 0x50000010
    Sub-VLANs (0 in total):
```

Table 20 Command output

Field	Description
Total 6 entries	Total number of (S, G) entries.
Multicast VLAN 10: Total 3 entries	Total number of (S, G) entries in multicast VLAN 10.
(0.0.0.0, 226.1.1.6)	(S, G) entry, where **0.0.0.0** in the S position means all multicast sources.

Flags	Entry flag.
	This field displays one flag or the sum of multiple flags. For example, the value 0x70000020 means that the entry has flags 0x20, 0x10000000, 0x20000000, and 0x40000000.
	The following flags are available for an entry:
	• **0x10**—The entry is created by the multicast VLAN.
	• **0x20**—The entry is created by the sub-VLAN of the multicast VLAN.
	• **0x40**—The entry is to be deleted.
	• **0x10000000**—This value represents one of the following situations:
	  o The entry is newly created.
	  o The device receives an IGMP query that matches the (S, G) entry but does not receive any matching IGMPv1 reports within an IGMP general query interval.
	• **0x20000000**—The device does not receive IGMPv2 or IGMPv3 reports that match the (S, G) entry within an IGMP general query interval.

Field	Description
	• **0x40000000**—The device does not receive IGMPv3 IS_EX (NULL) reports that match the (S, G) entry within an IGMP general query interval.
Sub-VLANs (1 in total)	Sub-VLAN list of the multicast VLAN, and the total number of the sub-VLANs.

Related commands

reset multicast-vlan group

multicast-vlan

Use **multicast-vlan** to configure a multicast VLAN and enter its view, or enter the view of an existing multicast VLAN.

Use **undo multicast-vlan** to remove the configuration of multicast VLANs.

Syntax

multicast-vlan *vlan-id*

undo multicast-vlan { **all** | *vlan-id* }

Default

No multicast VLANs exist.

Views

System view

Predefined user roles

network-admin

Parameters

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

all: Specifies all multicast VLANs.

Usage guidelines

The total number of multicast VLANs on a device cannot exceed the system upper limit.

You must enable IGMP snooping for the VLAN to be configured as a multicast VLAN.

Examples

Enable IGMP snooping for VLAN 100. Configure VLAN 100 as a multicast VLAN and enter its view.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 100
[Sysname-vlan100] igmp-snooping enable
[Sysname-vlan100] quit
[Sysname] multicast-vlan 100
[Sysname-mvlan-100]
```

Related commands

igmp-snooping enable

multicast-vlan entry-limit

Use **multicast-vlan entry-limit** to set the maximum number of multicast VLAN forwarding entries.

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

Syntax

multicast-vlan entry-limit *limit*

undo multicast-vlan entry-limit

Default

The maximum number of multicast VLAN forwarding entries is 4000.

Views

System view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of multicast VLAN forwarding entries, in the range of 0 to 4000.

Examples

Set the maximum number of multicast VLAN forwarding entries to 128.

```
<Sysname> system-view
[Sysname] multicast-vlan entry-limit 128
```

Related commands

entry-limit (IGMP-snooping view)

port (multicast-VLAN view)

Use **port** to assign user ports to a multicast VLAN.

Use **undo port** to delete user ports from a multicast VLAN.

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

Default

A multicast VLAN does not have user ports.

Views

Multicast VLAN view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number* to *interface-type interface-number*.

all: Specifies all user ports in the current multicast VLAN.

Usage guidelines

You can assign only Layer 2 Ethernet ports or Layer 2 aggregate interfaces to multicast VLANs. Additionally, you can assign a port to only one multicast VLAN.

For ports to be assigned to a multicast VLAN, you must enable IGMP snooping for the VLANs to which the ports belong.

Examples

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 as user ports to multicast VLAN 100.

```
<Sysname> system-view
[Sysname] multicast-vlan 100
[Sysname-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

port multicast-vlan

Use **port multicast-vlan** to assign a user port to a multicast VLAN.

Use **undo port multicast-vlan** to restore the default.

Syntax

port multicast-vlan *vlan-id*

undo port multicast-vlan

Default

A port does not belong to a multicast VLAN.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

You can assign a port to only one multicast VLAN.

For a port to be assigned to a multicast VLAN, you must enable IGMP snooping for the VLAN to which the port belongs.

Examples

Assign GigabitEthernet 1/0/1 as a user port to multicast VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port multicast-vlan 100
```

reset multicast-vlan group

Use **reset multicast-vlan group** to clear multicast groups in multicast VLANs.

Syntax

reset multicast-vlan group [*source-address* [**mask** { *mask-length* | *mask* }] | *group-address* [**mask** { *mask-length* | *mask* }] | **vlan** *vlan-id*] *

Views

User view

Predefined user roles

network-admin

Parameters

source-address: Specifies a multicast source by its IP address. If you do not specify a multicast source, this command clears multicast groups for all multicast sources in multicast VLANs.

mask { *mask-length | mask* }: Specifies a mask length or subnet mask for the multicast source address. The value range for the *mask-length* argument is 0 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

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 clears all multicast groups in multicast VLANs.

mask { *mask-length | mask* }: Specifies a mask length or subnet mask for the multicast group address. The value range for the *mask-length* argument is 4 to 32 (default), and the default value for the *mask* argument is 255.255.255.255.

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

Examples

Clear multicast groups for all multicast VLANs.

```
<Sysname> reset multicast-vlan group
```

Related commands

display multicast-vlan group

subvlan (multicast-VLAN view)

Use **subvlan** to assign VLANs as sub-VLANs to a multicast VLAN.

Use **undo subvlan** to delete sub-VLANs from a multicast VLAN.

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

Default

A multicast VLAN does not have sub-VLANs.

Views

Multicast VLAN view

Predefined user roles

network-admin

Parameters

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. The specified VLANs must exist and cannot be multicast VLANs or sub-VLANs of other multicast VLANs.

all: Specifies all sub-VLANs of the current multicast VLAN.

Usage guidelines

You must enable IGMP snooping for VLANs to be configured as sub-VLANs.

Examples

Assign VLAN 10 through VLAN 15 as sub-VLANs to multicast VLAN 100.

```
<Sysname> system-view
[Sysname] multicast-vlan 100
[Sysname-mvlan-100] subvlan 10 to 15
```

MLD snooping commands

display ipv6 l2-multicast fast-forwarding cache

Use **display ipv6 l2-multicast fast-forwarding cache** to display Layer 2 IPv6 multicast fast forwarding entries.

Syntax

display ipv6 l2-multicast fast-forwarding cache [**vlan** *vlan-id*] [*ipv6-source-address* | *ipv6-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.

ipv6-source-address: Specifies an IPv6 multicast source address. If you do not specify an IPv6 multicast source, this command displays Layer 2 IPv6 multicast forwarding entries for all IPv6 multicast sources.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays Layer 2 IPv6 multicast forwarding entries for all IPv6 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 IPv6 multicast fast forwarding entries for the master device.

Examples

Display Layer 2 IPv6 multicast fast forwarding entries.

```
<Sysname> display ipv6 l2-multicast fast-forwarding cache
Total 1 entries, 1 matched

(1::6, FF1E::2)
     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 21 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries in the Layer 2 IPv6 multicast fast forwarding table, and the total number of matching entries.
(1::6, FF1E::2)	(S, G) entry in the Layer 2 IPv6 multicast fast forwarding table.

Field	Description
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:
	• **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:
	• **0x1**—The port is added to the entry because of packets passed through between cards.
	• **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:
	• **Enabled**—Available.
	• **Disabled**—Unavailable.
Ingress port	Incoming port of the (S, G) entry.
List of 1 egress ports	List of outgoing ports of the (S, G) entry.

Related commands

reset ipv6 l2-multicast fast-forwarding cache all

display ipv6 l2-multicast ip

Use **display ipv6 l2-multicast ip** to display information about Layer 2 IPv6 multicast groups.

Syntax

display ipv6 l2-multicast ip [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. If you do not specify an IPv6 multicast group, this command displays information about all Layer 2 IPv6 multicast groups.

source *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about Layer 2 IPv6 multicast groups for all IPv6 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 IPv6 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 IPv6 multicast groups for VLAN 2.

```
<Sysname> display ipv6 l2-multicast ip vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
   (::, FF1E::101)
    Attribute: static, success
    Host ports (1 in total):
      GE1/0/1                              (S, SUC)
```

Table 22 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IPv6 multicast groups.
VLAN 2: Total 1 entries	Total number of Layer 2 IPv6 multicast groups in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 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 IPv6 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: • **D**—Dynamic port. • **S**—Static port. • **P**—IPv6 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 ipv6 l2-multicast ip forwarding

Use **display ipv6 l2-multicast ip forwarding** to display Layer 2 IPv6 multicast IP forwarding entries.

Syntax

display ipv6 l2-multicast ip forwarding [**group** *ipv6-group-address* | **source** *ipv6-source-address*] * [**vlan** *vlan-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group *ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. If you do not specify an IPv6 multicast group, this command displays Layer 2 IPv6 multicast IP forwarding entries for all IPv6 multicast groups.

source *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays Layer 2 IPv6 multicast IP forwarding entries for all IPv6 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 IPv6 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 IPv6 multicast IP forwarding entries for the master device.

Examples

Display Layer 2 IPv6 multicast IP forwarding entries for VLAN 2.

```
<Sysname> display ipv6 l2-multicast ip forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
   (::, FF1E::101)
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

Table 23 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IPv6 multicast IP forwarding entries.
VLAN 2: Total 1 entries	Total number of Layer 2 IPv6 multicast IP forwarding entries in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Host ports (3 in total)	Member ports and total number of member ports.

display ipv6 l2-multicast mac

Use **display ipv6 l2-multicast mac** to display information about Layer 2 IPv6 multicast MAC multicast groups.

Syntax

display ipv6 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 an IPv6 multicast MAC address. If you do not specify an IPv6 multicast MAC address, this command displays information about all Layer 2 IPv6 multicast 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 IPv6 multicast 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 IPv6 multicast MAC multicast groups for the master device.

Examples

Display information about Layer 2 IPv6 multicast MAC multicast groups for VLAN 2.

```
<Sysname> display ipv6 l2-multicast mac vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 3333-0000-0101
    Attribute: success
    Host ports (1 in total):
      GE1/0/1
```

Table 24 Command output

Field	Description
Total 1 entries	Total number of Layer 2 IPv6 MAC multicast groups.
VLAN 2: Total 1 entries	Total number of Layer 2 IPv6 MAC multicast groups in VLAN 2.
MAC group address	IPv6 address of the Layer 2 IPv6 MAC multicast group.
Attribute	Entry attribute: • **success**—Processing has succeeded. • **fail**—Processing has failed.
Host ports (1 in total)	Member ports and total number of member ports.

display ipv6 l2-multicast mac forwarding

Use **display ipv6 l2-multicast mac forwarding** to display Layer 2 IPv6 multicast MAC forwarding entries.

Syntax

display ipv6 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 an IPv6 MAC multicast group by its IPv6 MAC address. If you do not specify an IPv6 MAC multicast group, this command displays Layer 2 IPv6 multicast MAC forwarding entries for all IPv6 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 IPv6 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 IPv6 multicast MAC forwarding entries for the master device.

Examples

Display Layer 2 IPv6 multicast MAC forwarding entries for VLAN 2.

```
<Sysname> display ipv6 l2-multicast mac forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 3333-0000-0101
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

Table 25 Command output

Field	Description
Total 1 MAC entries	Total number of Layer 2 IPv6 multicast MAC forwarding entries.
VLAN 2: Total 1 entries	Total number of Layer 2 IPv6 multicast MAC forwarding entries in VLAN 2.
MAC group address	Address of the IPv6 MAC multicast group.
Host ports (3 in total)	Member ports, and the total number of member ports.

display mld-snooping

Use **display mld-snooping** to display MLD snooping status.

Syntax

display mld-snooping [**global** | **vlan** *vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

global: Displays the global MLD 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 MLD snooping status and the MLD snooping status in all VLANs.

Examples

Display the global MLD snooping status and the MLD snooping status for all VLANs.
```
<Sysname> display mld-snooping
MLD snooping information: Global
 Global-enable: Enabled
 Drop-unknown: Disabled
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
 Report-aggregation: Enabled
 Host-tracking: Disabled
 Dot1p-priority: --

MLD snooping information: VLAN 1
 MLD snooping: Enabled
 Drop-unknown: Disabled
 Version: 1
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
 Querier: Disabled
 Query-interval: 125s
 General-query source IP: FE80::2FF:FFFF:FE00:1
 Special-query source IP: FE80::2FF:FFFF:FE00:1
 Report source IP: FE80::2FF:FFFF:FE00:2
 Done source IP: FE80::2FF:FFFF:FE00:3
 Host-tracking: Disabled
 Dot1p-priority: 2
 Proxy: Disabled

MLD snooping information: VLAN 10
 MLD snooping: Enabled
 Drop-unknown: Enabled
 Version: 1
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-listener-query-interval: 1s
 Querier: Disabled
 Query-interval: 125s
 General-query source IP: FE80::2FF:FFFF:FE00:1
 Special-query source IP: FE80::2FF:FFFF:FE00:1
 Report source IP: FE80::2FF:FFFF:FE00:2
 Done source IP: FE80::2FF:FFFF:FE00:3
 Host-tracking: Disabled
 Dot1p-priority: --
```

75

```
Proxy: Disabled
```

Table 26 Command output

Field	Description
Global-enable	Global MLD snooping status: • Enabled. • Disabled.
MLD snooping	MLD snooping status in a VLAN: • **Enabled**. • **Disabled**. • **Globally enabled**. • **Inactive**—MLD snooping configuration does not take effect.
Drop-unknown	Status of dropping unknown IPv6 multicast data: • Enabled. • Disabled. • Globally enabled.
Version	MLD 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 time for responding to MLD general queries.
Last-listener-query-interval	Interval for sending MLD multicast-address-specific queries.
Report-aggregation	Status of MLD report suppression: • Enabled. • Disabled.
Dot1p-priority	802.1p priority for MLD messages. This field displays two hyphens (--) if the 802.1p priority is not configured.
Querier	Status of MLD snooping querier: • Enabled. • Disabled.
Query-interval	Interval for sending MLD general queries.
General-query source IP	Source IPv6 address of MLD general queries.
Special-query source IP	Source IPv6 address of MLD multicast-address-specific queries.
Report source IP	Source IPv6 address of MLD reports.
Done source IP	Source IPv6 address of MLD done messages.
Host-tracking	Status of host tracking: • Enabled. • Disabled. • Globally enabled.
Proxy	Status of MLD snooping proxying: • Enabled. • Disabled.

display mld-snooping group

Use **display mld-snooping group** to display information about dynamic MLD snooping group entries.

Syntax

display mld-snooping group [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays information about all dynamic MLD snooping group entries.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about dynamic MLD snooping group entries for all IPv6 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 MLD snooping group entries for all VLANs.

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

Examples

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

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

VLAN 2: Total 1 entries.
  (::,FF1E::101)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2                        (00:03:23)
```

Table 27 Command output

Field	Description
Total 1 entries	Total number of dynamic MLD snooping group entries.
VLAN 2: Total 1 entries	Total number of dynamic MLD snooping group entries in VLAN 2.

Field	Description
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Attribute	Entry attribute: • **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, but not on the member device for which the information is displayed.
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**—The entry does not exist.
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.
(00:03:23)	Remaining aging time for the dynamic member port. This field is always displayed for a global port (such as Layer 2 aggregate interfaces). For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

Related commands

reset mld-snooping group

display mld-snooping host-tracking

Use **display mld-snooping host-tracking** to display host tracking information.

Syntax

display mld-snooping host-tracking vlan *vlan-id* **group** *ipv6-group-address* [**source** *ipv6-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 *ipv6-group-address*: Specifies an IPv6 multicast group by its IPv6 address. The value range for the *ipv6-group-address* argument is FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

source *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this commands displays host tracking information for all IPv6 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 IPv6 multicast group FF1E::2 in VLAN 2.

```
<Sysname> display mld-snooping host-tracking vlan 2 group FF1E::2
VLAN 2
 (1::6, FF1E::2)
    Port: GE1/0/1
      Host                                   Uptime          Expires
      1::2                                    00:02:20        00:00:40
      1::3                                    00:02:21        00:00:39
```

Table 28 Command output

Field	Description
VLAN	VLAN ID.
(1::6, FF1E::2)	(S, G) entry, where 0::0 in the S position means any IPv6 multicast sources.
Port	Member port.
Host	IPv6 address of the host.
Uptime	Length of time elapsed since the host joined the IPv6 multicast group.
Expires	Remaining timeout time for the host. The host timeout time is the same as the aging timer of the port. The timer is reset when the port receives an MLD report from the host. This field displays **timeout** if the host times out.

Related commands

host-tracking (MLD-snooping view)

mld-snooping enable

mld-snooping host-tracking

display mld-snooping router-port

Use **display mld-snooping router-port** to display dynamic router port information.

Syntax

display mld-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 about dynamic router ports. If you do not specify this keyword, the command displays brief information about 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 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 mld-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 29 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. This field is always displayed for a global port (including Layer 2 aggregate interfaces). For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

Related commands

reset mld-snooping router-port

display mld-snooping static-group

Use **display mld-snooping static**-**group** to display information about static MLD snooping group entries.

Syntax

display mld-snooping static-**group** [*ipv6-group-address* | *ipv6-source-address*] * [**vlan** *vlan-id*] [**verbose**] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this

command displays information about static MLD snooping group entries for all IPv6 multicast groups.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about static MLD snooping group entries for all IPv6 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 MLD snooping group 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 a member device, this command displays information about static MLD snooping group entries for the master device.

Examples

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

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

VLAN 2: Total 1 entries.
  (::,FF1E::101)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2
```

Table 30 Command output

Field	Description
Total 1 entries	Total number of static MLD snooping group entries.
VLAN 2: Total 1 entries	Total number of static MLD snooping group entries in VLAN 2.
(::, FF1E::101)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Attribute	Entry attribute: • **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, but not on the member device for which the information is displayed.
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**—The entry does not exist.
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 mld-snooping static-router-port

Use **display mld-snooping static-router-port** to display static router port information.

Syntax

display mld-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 mld-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 mld-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 31 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 mld-snooping statistics

Use **display mld-snooping statistics** to display statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping.

Syntax

display mld-snooping statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display statistics for the MLD messages and IPv6 PIM hello messages learned through MLD snooping.

```
<Sysname> display mld-snooping statistics
Received MLD general queries:  0
Received MLDv1 specific queries:  0
Received MLDv1 reports:  0
Received MLD dones:  0
Sent     MLDv1 specific queries:  0
Received MLDv2 reports:  0
Received MLDv2 reports with right and wrong records:  0
Received MLDv2 specific queries:  0
Received MLDv2 specific sg queries:  0
Sent     MLDv2 specific queries:  0
Sent     MLDv2 specific sg queries:  0
Received IPv6 PIM hello:  0
Received error MLD messages:  0
```

Table 32 Command output

Field	Description
general queries	Number of MLD general queries.
specific queries	Number of MLD multicast-address-specific queries.
reports	Number of MLD reports.
dones	Number of MLD done messages.
reports with right and wrong records	Number of MLD reports with correct and incorrect records.
specific sg queries	Number of MLD multicast-address-and-source-specific queries.
IPv6 PIM hello	Number of IPv6 PIM hello messages.
error MLD messages	Number of MLD messages with errors.

Related commands

reset mld-snooping statistics

dot1p-priority (MLD-snooping view)

Use **dot1p-priority** to set the 802.1p priority for MLD messages globally.

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

Syntax

dot1p-priority *priority*

undo dot1p-priority

Default

The 802.1p priority for MLD messages is not configured. For MLD messages created by the device, the 802.1p priority is 0. For MLD messages to be forwarded, the device does not change the 802.1p priority.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

priority: Specifies an 802.1p priority for MLD 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 MLD-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 MLD messages to 3 globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] dot1p-priority 3
```

Related commands

mld-snooping dot1p-priority

drop-unknown (MLD-snooping view)

Use **drop-unknown** to enable dropping unknown IPv6 multicast data packets globally.

Use **undo drop-unknown** to disable dropping unknown IPv6 multicast data packets globally.

Syntax

drop-unknown

undo drop-unknown

Default

Dropping unknown IPv6 multicast data packets is disabled, and unknown IPv6 multicast data packets are flooded.

Views

MLD-snooping view

Predefined user roles

network-admin

Usage guidelines

You can enable this feature globally for all VLANs in MLD-snooping view or for a VLAN in VLAN view.

The **mld-snooping drop-unknown** command and the **drop-unknown** command in MLD-snooping view are mutually exclusive. You cannot configure them on the same device.

Examples

Enable dropping unknown IPv6 multicast data packets globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] drop-unknown
```

Related commands

mld-snooping drop-unknown

enable (MLD-snooping view)

Use **enable** to enable MLD snooping for multiple VLANs.

Use **undo enable** to disable MLD snooping for multiple VLANs.

Syntax

enable vlan *vlan-list*

undo enable vlan *vlan-list*

Default

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

Views

MLD-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 MLD snooping feature by using the **mld-snooping** command before you enable MLD snooping for multiple VLANs.

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

Examples

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

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

Related commands

mld-snooping

mld-snooping enable

entry-limit (MLD-snooping view)

Use **entry-limit** to globally set the maximum number of MLD 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 MLD snooping forwarding entries is 4294967295.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

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

Examples

Set the global maximum number of MLD snooping forwarding entries to 512.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] entry-limit 512
```

fast-leave (MLD-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

MLD-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 for all VLANs.

Usage guidelines

The fast-leave processing feature enables the device to immediately remove a port from the forwarding entry for an IPv6 multicast group when the port receives a done message.

You can enable fast-leave processing globally for all ports in MLD-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 MLD snooping fast-leave processing for VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] fast-leave vlan 2
```

Related commands

mld-snooping fast-leave

global-enable (MLD-Snooping view)

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

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

Syntax

global-enable

undo global-enable

Default

MLD snooping is disabled globally.

Usage guidelines

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

Views

MLD-snooping view

Predefined user roles

network-admin

Examples

Enable MLD snooping globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] global-enable
```

Related commands

enable (MLD-snooping view)

mld-snooping

mld-snooping disable

mld-snooping enable

group-policy (MLD-snooping view)

Use **group-policy** to globally configure an IPv6 multicast group policy to control the IPv6 multicast groups that hosts can join.

Use **undo group-policy** to globally delete IPv6 multicast group policies.

Syntax

group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

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

Default

No IPv6 multicast group policies exist. Hosts can join any IPv6 multicast groups.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic or advanced ACL by its number in the range of 2000 to 3999. Hosts can join only IPv6 multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join IPv6 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 for all VLANs.

Usage guidelines

An IPv6 multicast group policy filters MLD reports to control the IPv6 multicast groups that hosts can join.

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

You can configure an IPv6 multicast group policy globally for all ports in MLD-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 IPv6 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast group address.
- In an advanced ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast source address. The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group address.

  To match the following MLD reports, set the **source** *source-address source-prefix* option to 0::0:

  o MLDv1 reports.

  o MLDv2 IS_EX and MLDv2 TO_EX reports that do not carry IPv6 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 an IPv6 multicast group policy for VLAN 2 so that hosts in VLAN 2 can join only IPv6 multicast group FF03::101.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source ff03::101 128
[Sysname-acl-ipv6-basic-2000] quit
[Sysname] mld-snooping
[Sysname-mld-snooping] group-policy 2000 vlan 2
```

Related commands

mld-snooping group-policy

host-aging-time (MLD-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

MLD-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 MLD-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 IPv6 multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

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

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

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

Examples

Set the global aging timer for dynamic member ports to 300 seconds.

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

Related commands

mld-snooping host-aging-time

host-tracking (MLD-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

MLD-snooping view

Predefined user roles

network-admin

Usage guidelines

You can enable host tracking globally for all VLANs in MLD-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] mld-snooping
[Sysname-mld-snooping] host-tracking
```

Related commands

display mld-snooping host-tracking

mld-snooping host-tracking

last-listener-query-interval (MLD-snooping view)

Use **last-listener-query-interval** to set the MLD last listener query interval globally.

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

Syntax

last-listener-query-interval *interval*

undo last-listener-query-interval

Default

The MLD last listener query interval is 1 second.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD last listener 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 MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

Set the global MLD last listener query interval to 3 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] last-listener-query-interval 3
```

Related commands

mld-snooping last-listener-query-interval

max-response-time (MLD-snooping view)

Use **max-response-time** to set the maximum response time for MLD 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 MLD general queries is 10 seconds.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

You can set the time globally for all VLANs in MLD-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 IPv6 multicast group members, set the maximum response time for MLD general queries to be less than the MLD general query interval.

Examples

Set the global maximum response time for MLD general queries to 5 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] max-response-time 5
```

Related commands

mld-snooping max-response-time

mld-snooping query-interval

mld-snooping

Use **mld-snooping** to enable the MLD snooping feature and enter MLD-snooping view.

Use **undo mld-snooping** to disable the MLD snooping feature.

Syntax

> **mld-snooping**
>
> **undo mld-snooping**

Default

> The MLD snooping feature is globally disabled.

Views

> System view

Predefined user roles

> network-admin

Usage guidelines

> If you disable the MLD snooping feature, MLD snooping is disabled in all VLANs

Examples

> # Enable the MLD snooping feature and enter MLD-snooping view.
> ```
> <Sysname> system-view
> [Sysname] mld-snooping
> [Sysname-mld-snooping]
> ```

Related commands

> **enable** (MLD-snooping view)
>
> **mld-snooping enable**
>
> **mld-snooping disable**

mld-snooping disable

Use **mld-snooping disable** to disable MLD snooping for a VLAN.

Syntax

> **mld-snooping disable**

Default

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

Views

> VLAN view

Predefined user roles

> network-admin

Examples

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

Related commands

> **enable** (MLD-snooping view)
>
> **mld-snooping**
>
> **mld-snooping enable**

mld-snooping done source-ip

> Use **mld-snooping done source-ip** to configure the source IPv6 address for MLD done messages.
>
> Use **undo mld-snooping done source-ip** to restore the default.

Syntax

> **mld-snooping done source-ip** *ipv6-address*
>
> **undo mld-snooping done source-ip**

Default

> In a VLAN, the source IPv6 address of MLD done messages is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

Views

> VLAN view

Predefined user roles

> network-admin

Parameters

> *ipv6-address*: Specifies the source IPv6 address for MLD done messages.

Usage guidelines

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

Examples

> # In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address of MLD done messages.
>
> ```
> <Sysname> system-view
> [Sysname] mld-snooping
> [Sysname-mld-snooping] quit
> [Sysname] vlan 2
> [Sysname-vlan2] mld-snooping enable
> [Sysname-vlan2] mld-snooping done source-ip fe80:0:0:1::1
> ```

Related commands

> **enable** (MLD-snooping view)
>
> **mld-snooping enable**

mld-snooping dot1p-priority

> Use **mld-snooping dot1p-priority** to set the 802.1p priority for MLD messages in a VLAN.
>
> Use **undo mld-snooping dot1p-priority** to restore the default.

mld-snooping dot1p-priority *priority*

undo mld-snooping dot1p-priority

Default

The 802.1p priority for MLD messages is not configured. For MLD messages created by the device, the 802.1p priority is 0. For MLD messages to be forwarded, the device does not change the 802.1p priority.

Views

VLAN view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

You must enable MLD 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 MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

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

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

Related commands

dot1p-priority (MLD-snooping view)

enable (MLD-snooping view)

mld-snooping enable

mld-snooping drop-unknown

Use **mld-snooping drop-unknown** to enable dropping unknown IPv6 multicast data packets for a VLAN.

Use **undo mld-snooping drop-unknown** to disable dropping unknown IPv6 multicast data packets for a VLAN.

Syntax

mld-snooping drop-unknown

undo mld-snooping drop-unknown

Default

Dropping unknown IPv6 multicast data packets is disabled. Unknown IPv6 multicast data packets are flooded.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

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

You can enable this feature for a VLAN in VLAN view or globally for all VLANs in MLD-snooping view.

The **mld-snooping drop-unknown** command and the **drop-unknown** command in MLD-snooping view are mutually exclusive. You cannot configure them on the same device.

Examples

In VLAN 2, enable MLD snooping, and enable dropping unknown IPv6 multicast data packets.

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

Related commands

drop-unknown (MLD-snooping view)

enable (MLD-snooping view)

mld-snooping enable

mld-snooping enable

Use **mld-snooping enable** to enable MLD snooping for a VLAN.

Use **undo mld-snooping** to restore the MLD snooping status in a VLAN to the global MLD snooping status.

Syntax

mld-snooping enable

undo mld-snooping

Default

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

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

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

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

Examples

Enable the MLD snooping feature, and then enable MLD snooping for VLAN 2.

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

Related commands

enable (MLD-snooping view)

mld-snooping

mld-snooping disable

mld-snooping fast-leave

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

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

Syntax

mld-snooping fast-leave [**vlan** *vlan-list*]

undo mld-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 an IPv6 multicast group when the port receives a done message.

You can enable fast-leave processing for a port in interface view or globally for all ports in MLD-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] mld-snooping fast-leave vlan 2
```

Related commands

fast-leave (MLD-snooping view)

mld-snooping general-query source-ip

Use **mld-snooping general-query source-ip** to configure the source IPv6 address for MLD general queries.

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

Syntax

mld-snooping general-query source-ip *ipv6-address*

undo mld-snooping general-query source-ip

Default

In a VLAN, the source IPv6 address for MLD general queries is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD general queries.

Usage guidelines

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

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address for MLD general queries.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping general-query source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping group-limit

Use **mld-snooping group-limit** to set the maximum number of IPv6 multicast groups that a port can join.

Use **undo mld-snooping group-limit** to remove the limit on the maximum number of IPv6 multicast groups that a port can join.

Syntax

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

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

Default

No limit is placed on the maximum number of IPv6 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 for all VLANs.

Usage guidelines

This command takes effect only on the IPv6 multicast groups that a port joins dynamically.

Examples

On GigabitEthernet 1/0/1, set the maximum number to 10 for IPv6 multicast groups that the port can join in VLAN 2.

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

mld-snooping group-policy

Use **mld-snooping group-policy** to configure an IPv6 multicast group policy on a port to control the IPv6 multicast groups that hosts attached to the port can join.

Use **undo mld-snooping group-policy** to delete IPv6 multicast group policies on a port.

Syntax

mld-snooping group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

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

Default

No IPv6 multicast group policies exist. Hosts attached to the port can join any IPv6 multicast groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies an IPv6 basic or advanced ACL number in the range of 2000 to 3999. Hosts can join only the IPv6 multicast groups that the ACL permits. If the ACL does not exist or does not have valid rules, hosts cannot join IPv6 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

An IPv6 multicast group policy filters MLD reports to control the IPv6 multicast groups that hosts can join.

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

You can configure an IPv6 multicast group policy for a port in interface view or globally for all ports in MLD-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

When you configure a rule in the IPv6 ACL, follow these restrictions and guidelines:

- In a basic ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast group address.

- In an advanced ACL, the **source** *source-address source-prefix* option specifies an IPv6 multicast source address. The **destination** *dest-address dest-prefix* option specifies an IPv6 multicast group address.

  To match the following MLD reports, set the **source** *source-address source-prefix* option to 0::0:

  o MLDv1 reports.

  o MLDv2 IS_EX and MLDv2 TO_EX reports that do not carry IPv6 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 different VLANs on a port. If you configure multiple ACLs for the same VLANs on a port, the most recent configuration takes effect.

Examples

On GigabitEthernet 1/0/1, configure an IPv6 multicast group policy for VLAN 2 so that hosts attached to the port in VLAN 2 can join only the group FF03::101.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source ff03::101 128
[Sysname-acl-ipv6-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping group-policy 2000 vlan 2
```

Related commands

group-policy (MLD-snooping view)

mld-snooping host-aging-time

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

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

Syntax

mld-snooping host-aging-time *seconds*

undo mld-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 MLD 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 MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

To avoid mistakenly deleting IPv6 multicast group members, set the aging timer for dynamic member ports to be greater than the value calculated by using the following formula:

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

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

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

Examples

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

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

Related commands

enable (MLD-snooping view)

host-aging-time (MLD-snooping view)

mld-snooping enable

mld-snooping host-join

Use **mld-snooping host-join** to configure a port as a simulated member host for an IPv6 multicast group or an IPv6 multicast source and group.

Use **undo mld-snooping host-join** to remove the configuration of a simulated member host for an IPv6 multicast group.

Syntax

mld-snooping host-join *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

undo mld-snooping host-join { *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id* | **all** }

Default

A port is not a simulated member host of any IPv6 multicast groups or any IPv6 multicast sources and groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

source-ip *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you specify an IPv6 multicast source, this command configures the port as a simulated member host for an IPv6 multicast source and group. If you do not specify an IPv6 multicast source, this command configures the port as a simulated member host for an IPv6 multicast group. This option takes effect on MLDv2 snooping devices.

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

all: Specifies all IPv6 multicast groups and all IPv6 multicast sources and groups.

Usage guidelines

The version of MLD running on a simulated member host is the same as the version of MLD 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 for the IPv6 multicast group (*, FF3E::101) in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping host-join ff3e::101 vlan 2
```

mld-snooping host-tracking

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

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

Syntax

mld-snooping host-tracking

undo mld-snooping host-tracking

Default

Host tracking is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

You must enable MLD 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 MLD-snooping view. For a VLAN, the VLAN-specific configuration has the same priority as the global configuration.

Examples

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

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

Related commands

display mld-snooping host-tracking

host-tracking (MLD-snooping view)

mld-snooping enable

mld-snooping last-listener-query-interval

Use **mld-snooping last-listener-query-interval** to set the MLD last listener query interval for a VLAN.

Use **undo mld-snooping last-listener-query-interval** to restore the default.

Syntax

mld-snooping last-listener-query-interval *interval*

undo mld-snooping last-listener-query-interval

Default

The MLD last listener query interval is 1 second.

Views

VLAN view

Predefined user roles

network-admin

Parameters

interval: Specifies an MLD last listener query interval in the range of 1 to 25 seconds.

Usage guidelines

You must enable MLD 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 MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

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

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

Related commands

enable (MLD-snooping view)

last-listener-query-interval (MLD-snooping view)

mld-snooping enable

mld-snooping max-response-time

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

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

Syntax

mld-snooping max-response-time *seconds*

undo mld-snooping max-response-time

Default

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

Views

VLAN view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

You must enable MLD 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 MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration

To avoid mistakenly deleting IPv6 multicast group members, set the maximum response time for MLD general queries to be less than the MLD general query interval.

Examples

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

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
```

```
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping max-response-time 5
```

Related commands

enable (MLD-snooping view)

max-response-time (MLD-snooping view)

mld-snooping enable

mld-snooping query-interval

mld-snooping overflow-replace

Use **mld-snooping overflow-replace** to enable the IPv6 multicast group replacement feature on a port.

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

Syntax

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

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

Default

The IPv6 multicast group replacement feature 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 IPv6 multicast groups that a port joins dynamically.

You can enable the IPv6 multicast group replacement feature for a port in interface view or globally for all ports in MLD-snooping view. For a port, the port-specific configuration takes priority over the global configuration.

Examples

On GigabitEthernet 1/0/1, enable the IPv6 multicast group replacement feature for VLAN 2.

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

Related commands

overflow-replace (MLD-snooping view)

mld-snooping proxy enable

Use **mld-snooping proxy enable** to enable MLD snooping proxying for a VLAN.

Use **undo mld-snooping proxy enable** to disable MLD snooping proxying for a VLAN.

Syntax

mld-snooping proxy enable

undo mld-snooping proxy enable

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

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

This command does not take effect on a VLAN that is a sub-VLAN of an IPv6 multicast VLAN.

Examples

In VLAN 2, enable MLD snooping, and enable MLD snooping proxying.

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

Related commands

enable (MLD-snooping view)

mld-snooping enable

subvlan (IPv6 multicast-VLAN view)

mld-snooping querier

Use **mld-snooping querier** to enable the MLD snooping querier.

Use **undo mld-snooping querier** to disable the MLD snooping querier.

Syntax

mld-snooping querier

undo mld-snooping querier

Default

The MLD snooping querier is disabled.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

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

For a sub-VLAN of an IPv6 multicast VLAN, this command takes effect only after you remove the VLAN from the IPv6 multicast VLAN.

Examples

In VLAN 2, enable MLD snooping, and enable the MLD snooping querier.

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

Related commands

enable (MLD-snooping view)

mld-snooping enable

subvlan (IPv6 multicast-VLAN view)

mld-snooping query-interval

Use **mld-snooping query-interval** to set the MLD general query interval for a VLAN.

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

Syntax

mld-snooping query-interval *interval*

undo mld-snooping query-interval

Default

The MLD general query interval is 125 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

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

To avoid mistakenly deleting IPv6 multicast group members, set the MLD general query interval to be greater than the maximum response time for MLD general queries.

Examples

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

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
```

```
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping query-interval 20
```

Related commands

    enable (MLD-snooping view)

    max-response-time

    mld-snooping enable

    mld-snooping max-response-time

    mld-snooping querier

mld-snooping report source-ip

Use **mld-snooping report source-ip** to configure the source IPv6 address for MLD reports.

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

Syntax

mld-snooping report source-ip *ipv6-address*

undo mld-snooping report source-ip

Default

In a VLAN, the source IPv6 address for MLD reports is the IPv6 link-local address of the current VLAN interface. If the current VLAN interface does not have an IPv6 link-local address, the source IPv6 address is FE80::02FF:FFFF:FE00:0001.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD reports.

Usage guidelines

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

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address for MLD reports.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping report source-ip fe80:0:0:1::1
```

Related commands

    enable (MLD-snooping view)

    mld-snooping enable

mld-snooping router-aging-time

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

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

Syntax

mld-snooping router-aging-time *seconds*

undo mld-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 MLD 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 MLD-snooping view. For a VLAN, the VLAN-specific configuration takes priority over the global configuration.

Examples

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

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

Related commands

enable (MLD-snooping view)

mld-snooping enable

router-aging-time (MLD-snooping view)

mld-snooping router-port-deny

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

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

Syntax

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

undo mld-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.

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] mld-snooping router-port-deny vlan 2
```

mld-snooping source-deny

Use **mld-snooping source-deny** to enable IPv6 multicast source port filtering on a port to discard all IPv6 multicast data packets.

Use **undo mld-snooping source-deny** to disable IPv6 multicast source port filtering on a port.

Syntax

mld-snooping source-deny

undo mld-snooping source-deny

Default

IPv6 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 MLD-snooping view. For a port, the configuration in interface view has the same priority as the configuration in MLD-snooping view, and the most recent configuration takes effect.

Examples

Enable source port filtering for IPv6 multicast data on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping source-deny
```

Related commands

source-deny (MLD-snooping view)

mld-snooping special-query source-ip

Use **mld-snooping special-query source-ip** to configure the source IPv6 address for MLD multicast-address-specific queries.

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

Syntax

mld-snooping special-query source-ip *ipv6-address*

undo mld-snooping special-query source-ip

Default

In a VLAN, the source IPv6 address of MLD multicast-address-specific queries is one of the following:

- The source address of MLD general queries if the MLD snooping querier of the VLAN has received MLD general queries.
- The IPv6 link-local address of the current VLAN interface if the MLD snooping querier does not receive an MLD general query.
- FE80::02FF:FFFF:FE00:0001 if the MLD snooping querier does not receive an MLD general query and the current VLAN interface does not have an IPv6 link-local address.

Views

VLAN view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for MLD multicast-address-specific queries.

Usage guidelines

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

Examples

In VLAN 2, enable MLD snooping, and specify FE80:0:0:1::1 as the source IPv6 address of MLD multicast-address-specific queries.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping special-query source-ip fe80:0:0:1::1
```

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping static-group

Use **mld-snooping static-group** to configure a port as a static member port of an IPv6 multicast group or an IPv6 multicast source and group.

Use **undo mld-snooping static-group** to delete the configuration of static member ports.

Syntax

mld-snooping static-group *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

undo mld-snooping static-group { *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id* | **all** }

Default

A port is not a static member port of IPv6 multicast groups or any IPv6 multicast sources and groups.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

source-ip *ipv6-source-address*: Specifies an IPv6 multicast source by its IPv6 address. If you specify an IPv6 multicast source, this command configures the port as a static member port of an IPv6 multicast source and group. If you do not specify an IPv6 multicast source, this command configures the port as a static member port of an IPv6 multicast group. This option takes effect on MLDv2 snooping devices.

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

all: Specifies all IPv6 multicast groups and all IPv6 multicast sources and groups.

Examples

Configure GigabitEthernet 1/0/1 as a static member port for the IPv6 multicast group (*, FF3E::101) in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping static-group ff3e::101 vlan 2
```

mld-snooping static-router-port

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

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

Syntax

mld-snooping static-router-port vlan *vlan-id*

undo mld-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] mld-snooping static-router-port vlan 2
```

mld-snooping version

Use **mld-snooping version** to specify an MLD snooping version for a VLAN.

Use **undo mld-snooping version** to restore the default.

Syntax

mld-snooping version *version-number*

undo mld-snooping version

Default

The MLD snooping version in a VLAN is 1.

Views

VLAN view

Predefined user roles

network-admin

Parameters

version-number: Specifies an MLD snooping version, 1 or 2.

Usage guidelines

You must enable MLD snooping for a VLAN before you configure this command.

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

Examples

In VLAN 2, enable MLD snooping, and specify MLD snooping version 2.

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

Related commands

> **enable** (MLD-snooping view)
>
> **mld-snooping enable**
>
> **version** (MLD-snooping view)

overflow-replace (MLD-snooping view)

Use **overflow-replace** to enable the IPv6 multicast group replacement feature globally.

Use **undo overflow-replace** to disable the IPv6 multicast group replacement feature globally.

Syntax

> **overflow-replace** [**vlan** *vlan-list*]
>
> **undo overflow-replace** [**vlan** *vlan-list*]

Default

> The IPv6 multicast group replacement feature is disabled.

Views

> MLD-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 IPv6 multicast groups that a port joins dynamically.
>
> You can enable IPv6 multicast group replacement globally for all ports in MLD-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 IPv6 multicast group replacement feature for VLAN 2.
>
> ```
> <Sysname> system-view
> [Sysname] mld-snooping
> [Sysname-mld-snooping] overflow-replace vlan 2
> ```

Related commands

> **mld-snooping overflow-replace**

report-aggregation (MLD-snooping view)

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

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

Syntax

> **report-aggregation**
>
> **undo report-aggregation**

Default

MLD report suppression is enabled.

Views

MLD-snooping view

Predefined user roles

network-admin

Examples

Disable MLD report suppression.
```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] undo report-aggregation
```

reset ipv6 l2-multicast fast-forwarding cache

Use **reset ipv6 l2-multicast fast-forwarding cache** to clear Layer 2 IPv6 multicast fast forwarding entries.

Syntax

reset ipv6 l2-multicast fast-forwarding cache [**vlan** *vlan-id*] { { *ipv6-source-address* | *ipv6-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.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

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 IPv6 multicast fast forwarding entries for the master device.

all: Specifies all Layer 2 IPv6 multicast fast forwarding entries.

Examples

Clear all Layer 2 IPv6 multicast fast forwarding entries.
```
<Sysname> reset ipv6 l2-multicast fast-forwarding cache all
```

Clear the Layer 2 IPv6 multicast fast forwarding entry for the IPv6 group (*, FF1E::2).
```
<Sysname> reset ipv6 l2-multicast fast-forwarding cache FF1E::2
```

Related commands

display ipv6 l2-multicast fast-forwarding cache

reset mld-snooping group

Use **reset mld-snooping group** to clear information about dynamic MLD snooping group entries.

Syntax

reset mld-snooping group { *ipv6-group-address* [*ipv6-source-address*] | **all** } [**vlan** *vlan-id*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F.

ipv6-source-address: Specifies an IPv6 multicast source address. If you do not specify an IPv6 multicast source, this command clears information about dynamic MLD snooping group entries for all IPv6 multicast sources.

all: Specifies all IPv6 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 MLD snooping group entries for all VLANs.

Examples

Clear information about all dynamic MLD snooping group entries.

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

Related commands

display mld-snooping group

reset mld-snooping router-port

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

Syntax

reset mld-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 information about all dynamic router ports.

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

Related commands

display mld-snooping router-port

reset mld-snooping statistics

Use **reset mld-snooping statistics** to clear statistics for MLD messages and IPv6 PIM hello messages learned through MLD snooping.

Syntax

reset mld-snooping statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear statistics for all MLD messages and IPv6 PIM hello messages learned through MLD snooping.

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

Related commands

display mld-snooping statistics

router-aging-time (MLD-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

MLD-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 MLD-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] mld-snooping
[Sysname-mld-snooping] router-aging-time 100
```

116

Related commands

mld-snooping router-aging-time

source-deny (MLD-snooping view)

Use **source-deny** to enable IPv6 multicast source port filtering on ports to discard all IPv6 multicast data packets.

Use **undo source-deny** to disable IPv6 multicast source port filtering on ports.

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

Default

IPv6 multicast source port filtering is disabled.

Views

MLD-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 MLD-snooping view or for a port in interface view. For a port, the configuration in MLD-snooping view has the same priority as the configuration in interface view, and the most recent configuration takes effect.

Examples

Enable source port filtering for IPv6 multicast data on ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] source-deny port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Related commands

mld-snooping source-deny

version (MLD-snooping view)

Use **version** to specify an MLD 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 MLD snooping version in a VLAN is 1.

Views

MLD-snooping view

Predefined user roles

network-admin

Parameters

version-number: Specifies an MLD snooping version, 1 or 2.

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 MLD snooping for the specified VLANs before you execute this command.

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

Examples

Enable MLD snooping for VLAN 2 through VLAN 10, and specify MLD snooping version 2 for these VLANs.

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

Related commands

enable (MLD-snooping view)

mld-snooping enable

mld-snooping version

IPv6 PIM snooping commands

display ipv6 pim-snooping neighbor

Use **display ipv6 pim-snooping neighbor** to display IPv6 PIM snooping neighbor information.

Syntax

display ipv6 pim-snooping neighbor [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

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. If you do not specify a VLAN, this command displays IPv6 PIM snooping neighbor 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 IPv6 PIM snooping neighbor information for the master device.

verbose: Displays detailed information about IPv6 PIM snooping neighbors. If you do not specify this keyword, the command displays brief information about IPv6 PIM snooping neighbors.

Examples

Display detailed information about IPv6 PIM snooping neighbors for VLAN 2.

```
<Sysname> display ipv6 pim-snooping neighbor vlan 2 verbose
Total 2 neighbors.

VLAN 2: Total 2 neighbors.
  FE80::6401:101
    Slots (0 in total):
    Ports (1 in total):
      GE1/0/1                            (02:02:23)    LAN Prune Delay(T)
  FE80::C801:101
    Slots (0 in total):
    Ports (1 in total):
      GE1/0/2                            (02:02:25)
```

Table 33 Command output

Field	Description
Total 2 neighbors	Total number of IPv6 PIM snooping neighbors.
VLAN 2: Total 2 neighbors	Total number of IPv6 PIM snooping neighbors in VLAN 2.
FE80::6401:101	IPv6 address of the IPv6 PIM snooping neighbor.
Slots (0 in total)	Member IDs and total number of the member devices that have the neighbor, except for the specified member device or the master device when no member device is specified.
Ports (1 in total)	Ports where IPv6 PIM snooping neighbors reside, and the total number

Field	Description
	of the ports.
(02:02:23)	Remaining aging time for an IPv6 PIM snooping neighbor on the port. This field is always displayed for a global port (such as Layer 2 aggregate interfaces). For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
LAN Prune Delay	IPv6 PIM hello message sent by the IPv6 PIM snooping neighbor has the LAN_Prune_Delay option.
(T)	The join report suppression feature has been disabled for the IPv6 PIM snooping neighbor.

display ipv6 pim-snooping router-port

Use **display ipv6 pim-snooping router-port** to display IPv6 PIM snooping router port information.

Syntax

display ipv6 pim-snooping router-port [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

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. If you do not specify a VLAN, this command displays IPv6 PIM snooping router port information for all VLANs.

verbose: Displays detailed information about IPv6 PIM snooping router ports. If you do not specify this keyword, the command displays brief information about IPv6 PIM snooping 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 IPv6 PIM snooping router port information for the master device.

Examples

Display IPv6 PIM snooping router port information for VLAN 2.

```
<Sysname> display ipv6 pim-snooping router-port vlan 2
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1                           (00:01:30)
    GE1/0/2                           (00:01:32)
```

Table 34 Command output

Field	Description
VLAN 2	VLAN ID.
Router slots (0 in total)	Member IDs and total number of the member devices that have router ports, except for the specified member device or the master device when

Field	Description
	no member device is specified.
Router ports (2 in total)	Router ports and total number of router ports.
(00:01:30)	Remaining aging time for the router port. For a global port, this field is always displayed. For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

display ipv6 pim-snooping routing-table

Use **display ipv6 pim-snooping routing-table** to display IPv6 PIM snooping routing entries.

Syntax

display ipv6 pim-snooping routing-table [**vlan** *vlan-id*] [slot *slot-number*] [**verbose**]

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. If you do not specify a VLAN, this command displays IPv6 PIM snooping routing 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 IPv6 PIM snooping routing entries for the master device.

verbose: Displays detailed information about IPv6 PIM snooping routing entries. If you do not specify this keyword, the command displays brief information about IPv6 PIM snooping routing entries.

Examples

Display detailed information about IPv6 PIM snooping routing entries for VLAN 2.

```
<Sysname> display ipv6 pim-snooping routing-table vlan 2 verbose
Total 1 entries.
FSM Flag: NI-no info, J-join, PP-prune pending

VLAN 2: Total 1 entries.
  (2000::1, FF1E::1)
    FSM information: dummy
    Upstream neighbor: FE80::101
      Upstream Slots (0 in total):
      Upstream Ports (1 in total):
        GE1/0/1
      Downstream Slots (0 in total):
      Downstream Ports (2 in total):
        GE1/0/2
```

```
        Expires: 00:03:01, FSM: J
      Downstream Neighbors (2 in total):
        1001::1
          Expires: 00:59:19, FSM: J
        1001::2
          Expires: 00:59:20, FSM: J
    GE1/0/3
      Expires: 00:02:21, FSM: PP
```

Table 35 Command output

Field	Description
Total 1 entries	Total number of (S, G) and (*, G) entries.
FSM Flag: NI-no info, J-join, PP-prune pending	State machine flag of the downstream port: • **NI**—Initial state. • **J**—Join. • **PP**—Prune pending.
VLAN 2: Total 1 entries	Total number of (S, G) entries in VLAN 2.
(2000::1, FF1E::1)	(S, G) entry.
FSM information	Finite state machine information for the entry: • **delete**—The entry attributes have been deleted. • **dummy**—The entry is a new temporary entry. • **no info**—The entry does not exist.
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry.
Upstream Slots (0 in total)	Member IDs and total number of the member devices that have the upstream neighbor, except for the specified member device or the master device when no member device is specified.
Upstream Ports (1 in total)	Upstream ports, and the total number of the ports. This field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.
Downstream Slots (0 in total)	Member IDs and total number of the member devices that have downstream ports, except for the specified member device or the master device when no member device is specified.
Downstream Ports (2 in total)	Downstream ports of the upstream neighbor, and the total number of the ports.
Downstream Neighbors (2 in total)	Downstream neighbors of the downstream port, and the total number of the neighbors.
Expires: 00:03:01, FSM: J	Remaining aging time for the downstream port or downstream neighbor, and the finite sate machine information. For a global port, this field is always displayed. For a non-global port, this field is displayed when one of the following conditions exists: • The port is on the specified member device. • The port is on the master device and no member device is specified.

display ipv6 pim-snooping statistics

Use **display ipv6 pim-snooping statistics** to display statistics for the IPv6 PIM messages learned through IPv6 PIM snooping.

Syntax

display ipv6 pim-snooping statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display statistics for the IPv6 PIM messages learned through IPv6 PIM snooping.

```
<Sysname> display ipv6 pim-snooping statistics
Received IPv6 PIM hello:  100
Received IPv6 PIM join/prune:  100
Received IPv6 PIM error:  0
Received IPv6 PIM messages in total:  200
```

Table 36 Command output

Field	Description
Received IPv6 PIM hello	Number of received IPv6 PIM hello messages.
Received IPv6 PIM join/prune	Number of received IPv6 PIM join/prune messages.
Received IPv6 PIM error	Number of received IPv6 PIM messages with errors.
Received IPv6 PIM messages in total	Total number of received IPv6 PIM messages.

Related commands

reset ipv6 pim-snooping statistics

ipv6 pim-snooping enable

Use **ipv6 pim-snooping enable** to enable IPv6 PIM snooping for a VLAN.

Use **undo ipv6 pim-snooping enable** to disable IPv6 PIM snooping for a VLAN.

Syntax

ipv6 pim-snooping enable

undo ipv6 pim-snooping enable

Default

IPv6 PIM snooping is disabled for a VLAN.

Views

VLAN view

Predefined user roles

network-admin

Usage guidelines

IPv6 PIM snooping does not take effect on sub-VLANs of IPv6 multicast VLANs.

You must enable the MLD snooping feature and enable MLD snooping for a VLAN before you execute this command.

Examples

Enable the MLD snooping feature, and then enable MLD snooping and IPv6 PIM snooping for VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] ipv6 pim-snooping enable
```

Related commands

mld-snooping

mld-snooping enable

ipv6 pim-snooping graceful-restart join-aging-time

Use **ipv6 pim-snooping graceful-restart join-aging-time** to set the aging time for global downstream ports and global router ports on the new master device after a master/subordinate switchover.

Use **undo ipv6 pim-snooping graceful-restart join-aging-time** to restore the default.

Syntax

ipv6 pim-snooping graceful-restart join-aging-time *seconds*

undo ipv6 pim-snooping graceful-restart join-aging-time

Default

The default setting is 210 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging time in the range of 210 to 18000 seconds.

Usage guidelines

You must enable IPv6 PIM snooping for a VLAN before you execute this command.

Global ports include Layer 2 aggregate interfaces. A global downstream port or a global router port is a global port that acts as a downstream port or router port, respectively.

Examples

In VLAN 2, set the aging time to 300 seconds for global downstream ports and global router ports on the new master device after a master/subordinate switchover.

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

```
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] ipv6 pim-snooping enable
[Sysname-vlan2] ipv6 pim-snooping graceful-restart join-aging-time 300
```

Related commands

ipv6 pim-snooping enable

ipv6 pim-snooping graceful-restart neighbor-aging-time

Use **ipv6 pim-snooping graceful-restart neighbor-aging-time** to set the aging time for global neighbor ports on the new master device after a master/subordinate switchover.

Use **undo ipv6 pim-snooping graceful-restart neighbor-aging-time** to restore the default.

Syntax

ipv6 pim-snooping graceful-restart neighbor-aging-time *seconds*

undo ipv6 pim-snooping graceful-restart neighbor-aging-time

Default

The default setting is 105 seconds.

Views

VLAN view

Predefined user roles

network-admin

Parameters

seconds: Specifies an aging time in the range of 105 to 18000 seconds.

Usage guidelines

You must enable IPv6 PIM snooping for a VLAN before you execute this command.

Global ports include Layer 2 aggregate interfaces. A global neighbor port is a global port that acts as a neighbor port.

Examples

In VLAN 2, set the aging time to 300 seconds for global neighbor ports on the new master device after a master/subordinate switchover.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] ipv6 pim-snooping enable
[Sysname-vlan2] ipv6 pim-snooping graceful-restart neighbor-aging-time 300
```

Related commands

ipv6 pim-snooping enable

reset ipv6 pim-snooping statistics

Use **reset ipv6 pim-snooping statistics** to clear statistics for the IPv6 PIM messages learned through IPv6 PIM snooping.

Syntax

reset ipv6 pim-snooping statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear statistics for the IPv6 PIM messages learned through IPv6 PIM snooping.

```
<Sysname> reset ipv6 pim-snooping statistics
```

Related commands

display ipv6 pim-snooping statistics

IPv6 multicast VLAN commands

display ipv6 multicast-vlan

Use **display ipv6 multicast-vlan** to display information about IPv6 multicast VLANs.

Syntax

display ipv6 multicast-vlan [*vlan-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan-id: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, this command displays information about all IPv6 multicast VLANs.

Examples

Display information about all IPv6 multicast VLANs.

```
<Sysname> display ipv6 multicast-vlan
Total 2 IPv6 multicast VLANs.

IPv6 multicast VLAN 100:
  Sub-VLAN list(3 in total):
    2-3, 6
  Port list(3 in total):
    GE1/0/1
    GE1/0/2
    GE1/0/3

IPv6 multicast VLAN 200:
  Sub-VLAN list(0 in total):
  Port list(0 in total):
```

Table 37 Command output

Field	Description
Total 2 IPv6 multicast VLANs	Total number of IPv6 multicast VLANs.
Sub-VLAN list(3 in total)	Sub-VLAN list of the IPv6 multicast VLAN, and the total number of the sub-VLANs.
Port list(3 in total)	Port list of the IPv6 multicast VLAN, and the total number of the ports.

display ipv6 multicast-vlan forwarding-table

Use **display ipv6 multicast-vlan forwarding-table** to display IPv6 multicast VLAN forwarding entries.

Syntax

display ipv6 multicast-vlan forwarding-table [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **slot** *slot-number* | **subvlan** *vlan-id* | **vlan** *vlan-id*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays IPv6 multicast VLAN forwarding entries for all IPv6 multicast sources.

prefix-length: Specifies a prefix length of the IPv6 multicast source address. The value range is 0 to 128 and the default value is 128.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16, where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays IPv6 multicast VLAN forwarding entries for all IPv6 multicast groups.

prefix-length: Specifies a prefix length of the IPv6 multicast group address. The value range is 8 to 128 and the default value is 128.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 multicast VLAN forwarding entries for the master device.

subvlan *vlan-id*: Specifies a sub-VLAN by its VLAN ID. If you do not specify a sub-VLAN, this command displays IPv6 multicast VLAN forwarding entries for all sub-VLANs.

vlan *vlan-id*: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, this command displays IPv6 multicast VLAN forwarding entries for all VLANs.

Examples

Display all IPv6 multicast VLAN forwarding entries.

```
<Sysname> display ipv6 multicast-vlan forwarding-table
IPv6 multicast VLAN 100 Forwarding Table
Total 1 entries, 1 matched

00001. (1::1, FF0E::1)
     Flags: 0x10000
     IPv6 multicast VLAN: 100
     List of sub-VLANs (3 in total):
       1: VLAN 10
       2: VLAN 20
       3: VLAN 30
```

Table 38 Command output

Field	Description
IPv6 multicast VLAN 100 Forwarding Table	The multicast forwarding table for IPv6 multicast VLAN 100.
Total 1 entries, 1 matched	Total number of (S, G) entries, and the number of matching entries.
00001	Sequence number of the (S, G) entry.
(1::1, FF0E::1)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. In this example, the value 0x10000 means that the entry has only one flag 0x10000. The following flags are available for an entry: • **0x1**—The entry is in inactive state. • **0x4**—The entry fails to update. • **0x8**—The sub-VLAN information fails to update for the entry. • **0x200**—The entry is in GR state. • **0x10000**—The entry is an IPv6 multicast VLAN forwarding entry.
List of sub-VLANs (3 in total)	Sub-VLAN list of the IPv6 multicast VLAN, and the total number of the sub-VLANs.

display ipv6 multicast-vlan group

Use **display ipv6 multicast-vlan group** to display information about IPv6 multicast groups in IPv6 multicast VLANs.

Syntax

display ipv6 multicast-vlan group [*ipv6-source-address* | *ipv6-group-address* | **slot** *slot-number* | **verbose** | **vlan** *vlan-id*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command displays information about IPv6 multicast groups for all IPv6 multicast sources in IPv6 multicast VLANs.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command displays information about all IPv6 multicast groups in IPv6 multicast 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 IPv6 multicast groups in IPv6 multicast VLANs for the master device.

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

vlan *vlan-id*: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, this command displays information about IPv6 multicast groups for all IPv6 multicast VLANs.

Examples

Display detailed information about all IPv6 multicast groups in IPv6 multicast VLANs.

```
<Sysname> display ipv6 multicast-vlan group verbose
Total 6 entries.

IPv6 multicast VLAN 10: Total 3 entries.
  (2::2, FF0E::2)
    Flags: 0x70000020
    Sub-VLANs (1 in total):
      VLAN 40
  (22::22, FF0E::4)
    Flags: 0x70000030
    Sub-VLANs (1 in total):
      VLAN 40
  (::, FF0E::10)
    Flags: 0x10000030
    Sub-VLANs (1 in total):
      VLAN 40

IPv6 multicast VLAN 20: Total 3 entries.
  (2::2, FF0E::2)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (22::22, FF0E::4)
    Flags: 0x70000010
    Sub-VLANs (0 in total):
  (::, FF0E::10)
    Flags: 0x50000010
    Sub-VLANs (0 in total):
```

Table 39 Command output

Field	Description
Total 6 entries	Total number of (S, G) entries.
IPv6 multicast VLAN 10: Total 3 entries	Total number of (S, G) entries in IPv6 multicast VLAN 10.
(::, FF0E::10)	(S, G) entry, where a double colon (::) in the S position means all IPv6 multicast sources.
Flags	Entry flag. This field displays one flag or the sum of multiple flags. For example, the value 0x70000020 means that the entry has flags 0x20, 0x10000000, 0x20000000, and 0x40000000. The following flags are available for an entry: • **0x10**—The entry is created by the IPv6 multicast VLAN. • **0x20**—The entry is created by the sub-VLAN of the IPv6

Field	Description
	multicast VLAN.
	• **0x40**—The entry is to be deleted.
	• **0x10000000**—This value represents one of the following situations:
	○ The entry is newly created.
	○ The device receives an MLD query within an MLD general query interval.
	• **0x20000000**—The device does not receive MLDv1 or MLDv2 reports that match the entry within an MLD general query interval.
	• **0x40000000**—The device does not receive MLDv2 IS_EX (NULL) reports that match the entry within an MLD general query interval.
Sub-VLANs (1 in total)	Sub-VLAN list of the IPv6 multicast VLAN, and the total number of the sub-VLANs.

Related commands

> **reset ipv6 multicast-vlan group**

ipv6 multicast-vlan

Use **ipv6 multicast-vlan** to configure an IPv6 multicast VLAN and enter its view, or enter the view of an existing IPv6 multicast VLAN.

Use **undo ipv6 multicast-vlan** to remove the configuration of IPv6 multicast VLANs.

Syntax

> **ipv6 multicast-vlan** *vlan-id*
>
> **undo ipv6 multicast-vlan** { **all** | *vlan-id* }

Default

> No IPv6 multicast VLANs exist.

Views

> System view

Predefined user roles

> network-admin

Parameters

> *vlan-id*: Specifies an existing VLAN ID in the range of 1 to 4094.
>
> **all**: Specifies all IPv6 multicast VLANs.

Usage guidelines

> The total number of IPv6 multicast VLANs on a device cannot exceed the system upper limit.
>
> You must enable MLD snooping for the VLAN to be configured as an IPv6 multicast VLAN.

Examples

> # Enable MLD snooping for VLAN 100. Configure VLAN 100 as an IPv6 multicast VLAN and enter its view.
>
> ```
> <Sysname> system-view
> [Sysname] mld-snooping
> [Sysname-mld-snooping] quit
> ```

```
[Sysname] vlan 100
[Sysname-vlan100] mld-snooping enable
[Sysname-vlan100] quit
[Sysname] ipv6 multicast-vlan 100
[Sysname-ipv6-mvlan-100]
```

Related commands

mld-snooping enable

ipv6 multicast-vlan entry-limit

Use **ipv6 multicast-vlan entry-limit** to set the maximum number of IPv6 multicast VLAN forwarding entries.

Use **undo ipv6 multicast-vlan entry-limit** to restore the default.

Syntax

ipv6 multicast-vlan entry-limit *limit*

undo ipv6 multicast-vlan entry-limit

Default

The maximum number of IPv6 multicast VLAN forwarding entries is 2000.

Views

System view

Predefined user roles

network-admin

Parameters

limit: Specifies the maximum number of IPv6 multicast VLAN forwarding entries. The value range for this argument is 0 to 2000.

Examples

\# Set the maximum number of IPv6 multicast VLAN forwarding entries to 120.

```
<Sysname> system-view
[Sysname] ipv6 multicast-vlan entry-limit 120
```

Related commands

entry-limit (MLD-snooping view)

ipv6 port multicast-vlan

Use **ipv6 port multicast-vlan** to assign a user port to an IPv6 multicast VLAN.

Use **undo ipv6 port multicast-vlan** to restore the default.

Syntax

ipv6 port multicast-vlan *vlan-id*

undo ipv6 port multicast-vlan

Default

A port does not belong to an IPv6 multicast VLAN.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094.

Usage guidelines

You can assign a port to only one IPv6 multicast VLAN.

For the port to be assigned to an IPv6 multicast VLAN, you must enable MLD snooping for the VLAN to which the port belongs.

Examples

\# Assign GigabitEthernet 1/0/1 to IPv6 multicast VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 port multicast-vlan 100
```

port (IPv6 multicast VLAN view)

Use **port** to assign user ports to an IPv6 multicast VLAN.

Use **undo port** to delete user ports from an IPv6 multicast VLAN.

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

Default

An IPv6 multicast VLAN does not have user ports.

Views

IPv6 multicast VLAN view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number* to *interface-type interface-number*.

all: Specifies all user ports in the current IPv6 multicast VLAN.

Usage guidelines

You can assign only Layer 2 Ethernet interfaces or Layer 2 aggregate interfaces as user ports to an IPv6 multicast VLAN. Additionally, you can assign a port to only one IPv6 multicast VLAN.

For ports to be assigned to an IPv6 multicast VLAN, you must enable MLD snooping for the VLANs to which the ports belong.

Examples

\# Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 as user ports to IPv6 multicast VLAN 100.

```
<Sysname> system-view
[Sysname] ipv6 multicast-vlan 100
[Sysname-ipv6-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

reset ipv6 multicast-vlan group

Use **reset ipv6 multicast-vlan group** to clear IPv6 multicast group entries in IPv6 multicast VLANs.

Syntax

reset ipv6 multicast-vlan group [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **vlan** *vlan-id*] *

Views

User view

Predefined user roles

network-admin

Parameters

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers in the range of 0 to F. If you do not specify an IPv6 multicast group, this command clears all IPv6 multicast group entries in IPv6 multicast VLANs.

prefix-length: Specifies a prefix length of the IPv6 multicast group address. The value range is 8 to 128 and the default value is 128.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address. If you do not specify an IPv6 multicast source, this command clears IPv6 multicast group entries for all IPv6 multicast sources in IPv6 multicast VLANs.

prefix-length: Specifies a prefix length of the IPv6 multicast source address. The value range is 0 to 128 and the default value is 128.

vlan *vlan-id*: Specifies an IPv6 multicast VLAN by its VLAN ID in the range of 1 to 4094. If you do not specify an IPv6 multicast VLAN, this command clears IPv6 multicast group entries for all IPv6 multicast VLANs.

Examples

Clear all IPv6 multicast group entries for all IPv6 multicast VLANs.

```
<Sysname> reset ipv6 multicast-vlan group
```

Related commands

display ipv6 multicast-vlan group

subvlan (IPv6 multicast VLAN view)

Use **subvlan** to assign VLANs as sub-VLANs to an IPv6 multicast VLAN.

Use **undo subvlan** to delete sub-VLANs from an IPv6 multicast VLAN.

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

Default

An IPv6 multicast VLAN does not have sub-VLANs.

Views

IPv6 multicast VLAN view

Predefined user roles

network-admin

Parameters

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. The specified VLANs must exist and cannot be multicast VLANs or sub-VLANs of other IPv6 multicast VLANs.

all: Specifies all sub-VLANs of the current IPv6 multicast VLAN.

Usage guidelines

You must enable MLD snooping for VLANs to be configured as sub-VLANs of an IPv6 multicast VLAN.

Examples

Assign VLAN 10 through VLAN 15 as sub-VLANs to multicast VLAN 100.

```
<Sysname> system-view
[Sysname] ipv6 multicast-vlan 100
[Sysname-ipv6-mvlan-100] subvlan 10 to 15
```

Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x	y	... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x	y	...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x	y	... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x	y	...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
⚠ WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
△ CAUTION:	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
ⓘ IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
☀ TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)

- Product name, model or version, and serial number

- Operating system name and version

- Firmware version

- Error messages

- Product-specific reports and logs

- Add-on products or components

- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

- To download product updates, go to either of the following:

  o Hewlett Packard Enterprise Support Center **Get connected with updates** page:

    www.hpe.com/support/e-updates

  o Software Depot website:

    www.hpe.com/support/softwaredepot

- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

  ⓘ **IMPORTANT:**

  Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

Website	Link
Networking websites	
Hewlett Packard Enterprise Information Library for Networking	www.hpe.com/networking/resourcefinder
Hewlett Packard Enterprise Networking website	www.hpe.com/info/networking
Hewlett Packard Enterprise My Networking website	www.hpe.com/networking/support
Hewlett Packard Enterprise My Networking Portal	www.hpe.com/networking/mynetworking
Hewlett Packard Enterprise Networking Warranty	www.hpe.com/networking/warranty
General websites	
Hewlett Packard Enterprise Information Library	www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise Support Center	www.hpe.com/support/hpesc
Hewlett Packard Enterprise Support Services Central	ssc.hpe.com/portal/site/ssc/
Contact Hewlett Packard Enterprise Worldwide	www.hpe.com/assistance
Subscription Service/Support Alerts	www.hpe.com/support/e-updates
Software Depot	www.hpe.com/support/softwaredepot
Customer Self Repair (not applicable to all devices)	www.hpe.com/support/selfrepair
Insight Remote Support (not applicable to all devices)	www.hpe.com/info/insightremotesupport/docs

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title,

part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Index