

HP 5120 EI Switch Series

IP Multicast

Command Reference

Part number: 5998-1786

Software version: Release 2220

Document version: 6W100-20130810



Legal and notice information

© Copyright 2013 Hewlett-Packard Development Company, L.P.

No part of this documentation may be reproduced or transmitted in any form or by any means without prior written consent of Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Contents

IGMP snooping configuration commands	1
display igmp-snooping group	1
display igmp-snooping host	2
display igmp-snooping statistics	4
display mac-address multicast	5
dot1p-priority (IGMP-snooping view)	6
dscp (IGMP-snooping view)	7
fast-leave (IGMP-snooping view)	7
group-policy (IGMP-snooping view)	8
host-aging-time (IGMP-snooping view)	9
host-tracking (IGMP-snooping view)	10
igmp-snooping	10
igmp-snooping access-policy	11
igmp-snooping dot1p-priority	12
igmp-snooping drop-unknown	12
igmp-snooping enable	13
igmp-snooping fast-leave	14
igmp-snooping general-query source-ip	14
igmp-snooping group-limit	15
igmp-snooping group-policy	16
igmp-snooping host-aging-time	17
igmp-snooping host-join	18
igmp-snooping host-tracking	19
igmp-snooping last-member-query-interval	19
igmp-snooping leave source-ip	20
igmp-snooping max-response-time	21
igmp-snooping overflow-replace	22
igmp-snooping proxying enable	23
igmp-snooping querier	23
igmp-snooping query-interval	24
igmp-snooping report source-ip	25
igmp-snooping router-aging-time	25
igmp-snooping router-port-deny	26
igmp-snooping source-deny	27
igmp-snooping special-query source-ip	27
igmp-snooping static-group	28
igmp-snooping static-router-port	29
igmp-snooping version	30
last-member-query-interval (IGMP-snooping view)	31
mac-address multicast	31
max-response-time (IGMP-snooping view)	32
overflow-replace (IGMP-snooping view)	33
report-aggregation (IGMP-snooping view)	34
reset igmp-snooping group	34
reset igmp-snooping statistics	35
router-aging-time (IGMP-snooping view)	35
source-deny (IGMP-snooping view)	36

PIM snooping configuration commands	37
display pim-snooping neighbor	37
display pim-snooping routing-table	38
display pim-snooping statistics	39
pim-snooping enable	40
reset pim-snooping statistics	41
Multicast VLAN configuration commands	42
display multicast-vlan	42
multicast-vlan	43
port (multicast VLAN view)	44
port multicast-vlan	44
subvlan (multicast VLAN view)	45
MLD snooping configuration commands	46
display mld-snooping group	46
display mld-snooping host	47
display mld-snooping statistics	49
dot1p-priority (MLD-snooping view)	50
dscp (MLD-snooping view)	50
fast-leave (MLD-snooping view)	51
group-policy (MLD-snooping view)	52
host-aging-time (MLD-snooping view)	53
host-tracking (MLD-snooping view)	53
last-listener-query-interval (MLD-snooping view)	54
max-response-time (MLD-snooping view)	54
mld-snooping	55
mld-snooping access-policy	56
mld-snooping done source-ip	56
mld-snooping dot1p-priority	57
mld-snooping drop-unknown	58
mld-snooping enable	59
mld-snooping fast-leave	59
mld-snooping general-query source-ip	60
mld-snooping group-limit	61
mld-snooping group-policy	62
mld-snooping host-aging-time	63
mld-snooping host-join	64
mld-snooping host-tracking	65
mld-snooping last-listener-query-interval	65
mld-snooping max-response-time	66
mld-snooping overflow-replace	67
mld-snooping proxying enable	67
mld-snooping querier	68
mld-snooping query-interval	69
mld-snooping report source-ip	69
mld-snooping router-aging-time	70
mld-snooping router-port-deny	71
mld-snooping source-deny	72
mld-snooping special-query source-ip	72
mld-snooping static-group	73
mld-snooping static-router-port	74
mld-snooping version	75
overflow-replace (MLD-snooping view)	75
report-aggregation (MLD-snooping view)	76

reset mld-snooping group	77
reset mld-snooping statistics	77
router-aging-time (MLD-snooping view)	78
source-deny (MLD-snooping view)	78
IPv6 PIM snooping configuration commands	80
display pim-snooping ipv6 neighbor	80
display pim-snooping ipv6 routing-table	81
display pim-snooping ipv6 statistics	82
pim-snooping ipv6 enable	83
reset pim-snooping ipv6 statistics	84
IPv6 multicast VLAN configuration commands	85
display multicast-vlan ipv6	85
multicast-vlan ipv6	86
port (IPv6 multicast VLAN view)	87
port multicast-vlan ipv6	87
subvlan (IPv6 multicast VLAN view)	88
Support and other resources	89
Contacting HP	89
Subscription service	89
Related information	89
Documents	89
Websites	89
Conventions	90
Index	92

IGMP snooping configuration commands

display igmp-snooping group

Syntax

```
display igmp-snooping group [ vlan vlan-id ] [ slot slot-number ] [ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the IGMP snooping group information in the specified VLAN, where the *vlan-id* argument is in the range of 1 to 4094. If you do not specify a VLAN, this command displays the IGMP snooping group information in all VLANs.

slot *slot-number*: Displays the IGMP snooping group information on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

verbose: Displays the detailed IGMP snooping group information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display igmp-snooping group** to display IGMP snooping group information, including both dynamic entries and static entries.

Examples

Display detailed IGMP snooping group information in VLAN 2.

```
<Sysname> display igmp-snooping group vlan 2 verbose
Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):2.
Total 1 IP Group(s).
```

```

Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port(s).
    GE1/0/1                (D) ( 00:01:30 )
IP group(s):the following ip group(s) match to one mac group.
  IP group address:224.1.1.1
    (0.0.0.0, 224.1.1.1):
      Attribute:    Host Port
      Host port(s):total 1 port(s).
        GE1/0/2                (D) ( 00:03:23 )
MAC group(s):
  MAC group address:0100-5e01-0101
    Host port(s):total 1 port(s).
      GE1/0/2

```

Table 1 Command output

Field	Description
Total 1 IP Group(s).	Total number of IP multicast groups.
Total 1 IP Source(s).	Total number of multicast sources.
Total 1 MAC Group(s).	Total number of MAC multicast groups.
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port	Port flags: D —Dynamic port. S —Static port. C —Port copied from a (*, G) entry to an (S, G) entry. P —Port added by PIM snooping.
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R —Real egress sub-VLAN under the current entry. C —Sub-VLAN copied from a (*, G) entry to an (S, G) entry.
Router port(s)	Number of router ports.
(00:01:30)	Remaining time of the aging timer for the dynamic member port or router port.
IP group address	Address of IP multicast group.
(0.0.0.0, 224.1.1.1)	(S, G) entry, where 0.0.0.0 implies any multicast source.
MAC group address	Address of MAC multicast group.
Attribute	Attribute of IP multicast group.
Host port(s)	Number of member ports.

display igmp-snooping host

Syntax

```

display igmp-snooping host vlan vlan-id group group-address [ source source-address ] [ slot
slot-number ] [ | { begin | exclude | include } regular-expression ]

```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays information about the hosts tracked by IGMP snooping in the specified VLAN, where *vlan-id* is in the range of 1 to 4094.

group *group-address*: Displays information about the hosts tracked by IGMP snooping that are in the specified IGMP snooping group. The value of *group-address* ranges from 224.0.1.0 to 239.255.255.255.

source *source-address*: Displays information about the hosts tracked by IGMP snooping that are in the specified multicast source, where *source-address* is a valid unicast address or 0.0.0.0. A source IP address of 0.0.0.0 specifies all multicast sources.

slot *slot-number*: Displays information about the hosts tracked by IGMP snooping on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display igmp-snooping host** to display information about the hosts tracked by IGMP snooping.

Examples

Display information about the hosts tracked by IGMP snooping in VLAN 2 that are in multicast group 224.1.1.1.

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

```
VLAN(ID) : 2
```

```
(0.0.0.0, 224.1.1.1)
```

```
Port : GigabitEthernet1/0/1
```

```
Host
```

```
Uptime
```

```
Expires
```

```
1.1.1.1
```

```
00:02:20
```

```
00:00:40
```

```
2.2.2.2
```

```
00:02:21
```

```
00:00:39
```

```
Port : GigabitEthernet1/0/2
```

```
Host
```

```
Uptime
```

```
Expires
```

```
3.3.3.3
```

```
00:02:20
```

```
00:00:40
```

Table 2 Command output

Field	Description
(0.0.0.0, 224.1.1.1)	(S, G) entry, where 0.0.0.0 indicates all multicast sources

Field	Description
Port	Member port
Host	Host IP address
Uptime	Host running duration
Expires	Host expiration time, where <i>timeout</i> means that the host has expired

display igmp-snooping statistics

Syntax

display igmp-snooping statistics [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display igmp-snooping statistics** to display statistics for IGMP messages learned through IGMP snooping.

Examples

Display statistics for IGMP 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 error IGMP messages:19.
```

Table 3 Command output

Field	Description
general queries	General query messages
specific queries	Group-specific query messages
reports	Report messages
leaves	Leave messages
reports with right and wrong records	Report messages with correct and incorrect records
specific sg query packet(s)	Group-and-source-specific query message or messages
error IGMP messages	IGMP messages with errors

display mac-address multicast

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [**multicast**] [**vlan** *vlan-id*] [**count**]] [{ **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

mac-address: Displays the multicast MAC address entry for the specified MAC address. The MAC address can be any multicast MAC address except 0100-5Exx-xxxx and 3333-xxxx-xxxx, where x represents an arbitrary hexadecimal number from 0 to F. A multicast MAC address is a MAC address whose the least significant bit of the most significant octet is 1.

vlan *vlan-id*: Displays multicast MAC address entries for the specified VLAN, where *vlan-id* is in the range of 1 to 4094. If you do not specify a VLAN, this command displays the static multicast MAC address entries for all VLANs.

multicast: Displays static multicast MAC address entries.

count: Displays the number of matched static multicast MAC address entries. With this argument specified, the number of matched static multicast MAC address entries is displayed, without displaying any content of the matched entries.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

With no parameters specified or with only **vlan**, **count**, or both of them specified, this command displays all MAC address table entries, including static multicast MAC address entries and unicast MAC address entries.

Related commands: **mac-address multicast**; **display mac-address** (*Layer 2—LAN Switching Command Reference*).

Examples

Display the static multicast MAC address entries for VLAN 2.

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

MAC ADDR	VLAN ID	STATE	PORT INDEX	AGING TIME(s)
0100-0001-0001	2	Multicast	GigabitEthernet1/0/1	NOAGED
			GigabitEthernet1/0/2	
			GigabitEthernet1/0/3	
			GigabitEthernet1/0/4	

```

--- 1 mac address(es) found ---

```

Table 4 Command output

Field	Description
MAC ADDR	MAC address.
VLAN ID	ID of the VLAN to which the network device identified by the MAC address belongs.
STATE	Status of the MAC address; multicast indicates a static multicast MAC address entry.
PORT INDEX	Outgoing ports of the multicast MAC address entry.
AGING TIME(s)	State of the aging timer. The aging timer for static multicast MAC addresses has only one state NOAGED , which indicates that this entry never expires.
1 mac address(es) found	One static multicast MAC address entry is found.

dot1p-priority (IGMP-snooping view)

Syntax

dot1p-priority *priority-number*

undo dot1p-priority

View

IGMP-snooping view

Default level

2: System level

Parameters

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

Description

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

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

The default 802.1p precedence for IGMP messages is 0.

Examples

Set the 802.1p precedence for IGMP messages to 3 globally.

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

dscp (IGMP-snooping view)

Syntax

dscp *dscp-value*
undo dscp

View

IGMP-snooping view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value for IGMP messages, in the range of 0 to 63.

Description

Use **dscp** to set the DSCP value for IGMP messages.

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

The default DSCP value in IGMP messages is 48.

This command applies to only the IGMP messages that the local switch generates when the switch or its port acts as a member host, rather than those forwarded ones.

Examples

Set the DSCP value to 63 for IGMP messages.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dscp 63
```

fast-leave (IGMP-snooping view)

Syntax

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

View

IGMP-snooping view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command takes effect for all VLANs. If you specify one or more VLANs, the command takes effect for the specified VLANs only.

Description

Use **fast-leave** to enable fast-leave processing globally. With this function enabled, when the switch receives an IGMP leave message on a port, it directly removes that port from the multicast forwarding entry of the specific group.

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

By default, fast-leave processing is disabled.

This command takes effect in IGMP snooping-enabled VLANs.

Related commands: **igmp-snooping fast-leave**.

Examples

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

group-policy (IGMP-snooping view)

Syntax

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

View

IGMP-snooping view

Default level

2: System level

Parameters

acl-number: Specifies a basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule matches the multicast source addresses specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX or TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command takes effect for all VLANs. If you specify one or more VLANs, the command takes effect for the specified VLANs only.

Description

Use **group-policy** to configure a global multicast group filter, namely, to control the multicast groups that a host can join.

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

By default, no global multicast group filter is configured. Namely, a host can join any valid multicast group.

If the specified ACL does not exist or the ACL rule is null, all multicast groups are filtered out.

You can configure different ACL rules for a port in different VLANs. For a given VLAN, a newly configured ACL rule overrides the existing one.

Related commands: **igmp-snooping group-policy**.

Examples

Apply ACL 2000 as a multicast group filter in VLAN 2 so that hosts in this VLAN can join 225.1.1.1 only.

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

host-aging-time (IGMP-snooping view)

Syntax

host-aging-time *interval*

undo host-aging-time

View

IGMP-snooping view

Default level

2: System level

Parameters

interval: Specifies an aging timer in seconds for dynamic member ports. The value ranges from 200 to 1000.

Description

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

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

By default, the aging timer of a dynamic member port is 260 seconds.

This command takes effect only in IGMP snooping-enabled VLANs.

Related commands: **igmp-snooping host-aging-time**.

Examples

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

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

host-tracking (IGMP-snooping view)

Syntax

host-tracking
undo host-tracking

View

IGMP-snooping view

Default level

2: System level

Parameters

None

Description

Use **host-tracking** to enable the IGMP snooping host tracking function globally.

Use **undo host-tracking** to disable the IGMP snooping host tracking function globally.

By default, this function is disabled.

This command takes effect only in IGMP snooping-enabled VLANs.

Related commands: **display igmp-snooping host** and **igmp-snooping host-tracking**.

Examples

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

igmp-snooping

Syntax

igmp-snooping
undo igmp-snooping

View

System view

Default level

2: System level

Parameters

None

Description

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

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

By default, IGMP snooping is disabled.

Related commands: **igmp-snooping enable**.

Examples

Enable IGMP snooping globally and enter IGMP-snooping view.

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

igmp-snooping access-policy

Syntax

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

View

User profile view

Default level

2: System level

Parameters

acl-number: Specifies a basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL matches the multicast source address or addresses specified in IGMPv3 reports, rather than the source addresses of the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX and TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

all: Specifies all ACLs.

Description

Use **igmp-snooping access-policy** to configure a multicast user control policy.

Use **undo igmp-snooping access-policy** to remove the configuration.

By default, no user control policy is configured. Namely, a user can join any valid multicast group.

You can use this command repeatedly to configure multiple multicast user control policies.

Only the S3100V2-EI switches support multicast user control policies.

Examples

Create and enable a user profile named **abc** to allow users to join 225.1.1.1 only.

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


igmp-snooping dot1p-priority

Syntax

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

View

VLAN view

Default level

2: System level

Parameters

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

Description

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

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

The default 802.1p precedence for the IGMP messages in a VLAN is 0.

Before you configure this command in a VLAN, enable IGMP snooping in the VLAN.

Related commands: **igmp-snooping enable**.

Examples

```
# Enable IGMP snooping in VLAN 2 and set the 802.1p precedence for the IGMP messages in the VLAN 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
```

igmp-snooping drop-unknown

Syntax

```
igmp-snooping drop-unknown  
undo igmp-snooping drop-unknown
```

View

VLAN view

Default level

2: System level

Parameters

None

Description

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

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

By default, this function is disabled. That is, unknown multicast data is flooded.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**.

Examples

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

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

igmp-snooping enable

Syntax

igmp-snooping enable

undo igmp-snooping enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

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

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

By default, IGMP snooping is disabled in a VLAN.

IGMP snooping must be enabled globally before it can be enabled in a VLAN.

Related commands: **igmp-snooping**.

Examples

Enable IGMP snooping in VLAN 2.

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

igmp-snooping fast-leave

Syntax

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

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **igmp-snooping fast-leave** to enable fast-leave processing on the current port or group of ports. With this function enabled, when the switch receives an IGMP leave message on a port, it directly removes that port from the multicast forwarding entry of the specific group.

Use **undo igmp-snooping fast-leave** to disable fast-leave processing on the current port or group of ports.

By default, fast-leave processing is disabled.

This command takes effect in IGMP snooping-enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **fast-leave**.

Examples

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

igmp-snooping general-query source-ip

Syntax

```
igmp-snooping general-query source-ip { ip-address | current-interface }  
undo igmp-snooping general-query source-ip
```

View

VLAN view

Default level

2: System level

Parameters

ip-address: Specifies the source address of IGMP general queries, which can be any legal IP address.

current-interface: Sets the source address of IGMP general queries to the address of the current VLAN interface. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 is used as the source IP address of IGMP general queries.

Description

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

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

By default, the source IP address of IGMP general queries is 0.0.0.0.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**.

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
```

igmp-snooping group-limit

Syntax

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

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

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

limit: Specifies the maximum number of multicast groups that a port can join. in the range of 1 to 1000.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

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

Use **undo igmp-snooping group-limit** to restore the default.

By default, the upper limit is 1000.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Examples

```
# Specify to allow GigabitEthernet 1/0/1 in VLAN 2 to join up to 10 multicast groups.
```

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

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-limit 10 vlan 2
```

igmp-snooping group-policy

Syntax

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

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

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

acl-number: Specifies a basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule matches the multicast source address or addresses specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX and TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

vlan vlan-list: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

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

Use **undo igmp-snooping group-policy** to remove a multicast group filter.

By default, no multicast group filter is configured on an interface. Namely, a host can join any valid multicast group.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

If the specified ACL does not exist or the ACL rule is null, all multicast groups are filtered out.

You can configure different ACL rules for a port in different VLANs. For a given VLAN, a newly configured ACL rule overrides the existing one.

Related commands: **group-policy**.

Examples

Apply ACL 2000 as a multicast group filter so that hosts on GigabitEthernet 1/0/1 in VLAN 2 can join 225.1.1.1 only.

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

igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *interval*

undo igmp-snooping host-aging-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an aging timer in seconds for dynamic member ports. The value ranges from 200 to 1000.

Description

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

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

By default, the aging time of a dynamic member port is 260 seconds.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **host-aging-time** and **igmp-snooping enable**.

Examples

Enable IGMP snooping and set the aging timer for dynamic member ports in VLAN 2 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

```

igmp-snooping host-join

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*

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

group-address: Specifies the address of the multicast group that the simulated host will join, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Specifies the address of the multicast source that the simulated host will join. The value of this argument should be a valid unicast address or 0.0.0.0. A source IP address of 0.0.0.0 specifies all multicast sources.

vlan *vlan-id*: Specifies the VLAN that comprises the ports, where *vlan-id* is in the range of 1 to 4094.

Description

Use **igmp-snooping host-join** to enable simulated joining on a port. That is, you configure the port as a simulated member host for the specified multicast group or source and group.

Use **undo igmp-snooping host-join** to remove the simulated member hosts from the specified multicast group or source and group.

By default, this function is disabled.

This command takes effect in IGMP snooping-enabled VLANs. The IGMP version on the simulated member host is consistent with the version of IGMP snooping that is running in the VLAN.

The **source-ip** *source-address* option in the command is meaningful only for IGMPv3 snooping. If IGMPv2 snooping is running, the **source-ip** *source-address* option does not take effect although you can include **source-ip** *source-address* in the command.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN.

In port group view, this command takes effect only on the ports in this port group that belong to the specified VLAN.

Examples

Configure GigabitEthernet 1/0/1 as a simulated member host in VLAN 2 for multicast source 1.1.1.1 and multicast group 232.1.1.1.

```

<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

Syntax

igmp-snooping host-tracking

undo igmp-snooping host-tracking

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping host-tracking** to enable the IGMP snooping host tracking function in a VLAN.

Use **undo igmp-snooping host-tracking** to disable the IGMP snooping host tracking function in a VLAN.

By default, this function is disabled.

Before you configure this command, enable IGMP snooping in the VLAN first.

Related commands: **display igmp-snooping host**, **host-tracking**, and **igmp-snooping enable**.

Examples

Enable IGMP snooping and IGMP snooping host tracking 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 host-tracking

```

igmp-snooping last-member-query-interval

Syntax

igmp-snooping last-member-query-interval *interval*

undo igmp-snooping last-member-query-interval

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies the IGMP last-member query interval in seconds. The value ranges from 1 to 5.

Description

Use **igmp-snooping last-member-query-interval** to set the IGMP last-member query interval in the VLAN.

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

By default, the IGMP last-member query interval is 1 second.

The IGMP last-member query interval determines the interval for sending IGMP group-specific queries and the maximum response delay for IGMP group-specific queries in a VLAN.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable** and **last-member-query-interval**.

Examples

Enable IGMP snooping and set the IGMP last-member query interval to 3 seconds 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 last-member-query-interval 3
```

igmp-snooping leave source-ip

Syntax

igmp-snooping leave source-ip { *ip-address* | **current-interface** }

undo igmp-snooping leave source-ip

View

VLAN view

Default level

2: System level

Parameters

ip-address: Specifies a source address for the IGMP leave messages that the IGMP snooping proxy sends, which can be any legal IP address.

current-interface: Specifies the IP address of the current VLAN interface as the source address of IGMP leave messages that the IGMP snooping proxy sends. If no IP address has been assigned to the current VLAN interface, the default IP address 0.0.0.0 is used.

Description

Use **igmp-snooping leave source-ip** to configure the source IP address of the IGMP leave messages that the IGMP snooping proxy sends.

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

By default, the source IP address of the IGMP leave messages that the IGMP snooping proxy sends is 0.0.0.0.

Before you configure this command in a VLAN, enable IGMP snooping in the VLAN.

The source IP address configured in the **igmp-snooping leave source-ip** command also applies when the simulated host sends IGMP leave messages.

Related commands: **igmp-snooping enable**.

Examples

Enable IGMP snooping in VLAN 2 and configure the source IP address of IGMP leave messages that the IGMP snooping proxy sends in VLAN 2 to 10.1.1.1.

```
<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
```

igmp-snooping max-response-time

Syntax

igmp-snooping max-response-time *interval*

undo igmp-snooping max-response-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for IGMP general queries in seconds. The value ranges from 1 to 25.

Description

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

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

By default, the maximum response delay for IGMP general queries is 10 seconds.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**, **igmp-snooping query-interval**, and **max-response-time**.

Examples

Enable IGMP snooping and set the maximum response delay for IGMP general queries to 5 seconds 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 max-response-time 5
```

igmp-snooping overflow-replace

Syntax

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

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

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

Use **undo igmp-snooping overflow-replace** to disable the multicast group replacement function.

By default, the multicast group replacement function is disabled.

This command takes effect in IGMP snooping-enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **overflow-replace**.

Examples

Enable the multicast group replacement function on GigabitEthernet 1/0/1 in VLAN 2.

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

igmp-snooping proxying enable

Syntax

igmp-snooping proxying enable
undo igmp-snooping proxying enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping proxying enable** to enable the IGMP snooping proxying function in a VLAN.

Use **undo igmp-snooping proxying enable** to disable the IGMP snooping proxying function in a VLAN.

By default, IGMP snooping proxying is disabled in all VLANs.

Before you configure this command in a VLAN, enable IGMP snooping in the VLAN.

Related commands: **igmp-snooping enable**.

Examples

Enable IGMP snooping and then IGMP snooping proxying 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 proxying enable
```

igmp-snooping querier

Syntax

igmp-snooping querier
undo igmp-snooping querier

View

VLAN view

Default level

2: System level

Parameters

None

Description

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

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

By default, the IGMP snooping querier function is disabled.

This command takes effect only if IGMP snooping is enabled in the VLAN.

This command does not take effect in a sub-VLAN of a multicast VLAN.

Related commands: **igmp-snooping enable** and **subvlan**.

Examples

Enable IGMP snooping and the IGMP snooping querier function 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 querier
```

igmp-snooping query-interval

Syntax

igmp-snooping query-interval *interval*

undo igmp-snooping query-interval

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an interval in seconds for sending IGMP general queries. The value ranges from 2 to 300.

Description

Use **igmp-snooping query-interval** to configure the interval for sending IGMP general queries.

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

By default, the IGMP general query interval is 60 seconds.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**, **igmp-snooping max-response-time**, **igmp-snooping querier**, and **max-response-time**.

Examples

Enable IGMP snooping and set the interval for sending IGMP general queries to 20 seconds 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 query-interval 20
```

igmp-snooping report source-ip

Syntax

igmp-snooping report source-ip { *ip-address* | **current-interface** }

undo igmp-snooping report source-ip

View

VLAN view

Default level

2: System level

Parameters

ip-address: Specifies a source address for the IGMP reports that the IGMP snooping proxy sends. The address can be any legal IP address.

current-interface: Specifies the IP address of the current VLAN interface as the source address of IGMP reports that the IGMP snooping proxy sends. If no IP address has been assigned to the current VLAN interface, the default IP address 0.0.0.0 is used.

Description

Use **igmp-snooping report source-ip** to configure the source IP address of the IGMP reports that the IGMP snooping proxy sends.

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

By default, the source IP address of the IGMP reports that the IGMP snooping proxy sends is 0.0.0.0.

Before you configure this command in a VLAN, enable IGMP snooping in the VLAN.

The source IP address configured in the **igmp-snooping report source-ip** command also applies when the simulated host sends IGMP reports.

Related commands: **igmp-snooping enable**.

Examples

Enable IGMP snooping in VLAN 2 and configure the source IP address of IGMP reports that the IGMP snooping proxy sends in VLAN 2 to 10.1.1.1.

```
<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
```

igmp-snooping router-aging-time

Syntax

igmp-snooping router-aging-time *interval*

undo igmp-snooping router-aging-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an aging timer for dynamic router ports in seconds. The value ranges from 1 to 1000.

Description

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

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

By default, the aging timer of a dynamic router port is 105 seconds.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable** and **router-aging-time**.

Examples

Enable IGMP snooping and set the aging timer for dynamic router ports to 100 seconds 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 router-aging-time 100
```

igmp-snooping router-port-deny

Syntax

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

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

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

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

Use **undo igmp-snooping router-port-deny** to restore the default.

By default, a port can become a dynamic router port.

This command take effects in IGMP snooping-enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or more VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or more VLANs, the command takes effect only on those ports in this group that belong to the specified 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] igmp-snooping router-port-deny vlan 2
```

igmp-snooping source-deny

Syntax

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

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **igmp-snooping source-deny** to enable multicast source port filtering.

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

By default, multicast source port filtering is disabled.

This command takes effect in IGMP snooping-enabled VLANs.

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
```

igmp-snooping special-query source-ip

Syntax

igmp-snooping special-query source-ip { ip-address | current-interface }
undo igmp-snooping special-query source-ip

View

VLAN view

Default level

2: System level

Parameters

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

current-interface: Specifies the address of the current VLAN interface as the source address of IGMP group-specific queries. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 is used as the source IP address of IGMP group-specific queries.

Description

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.

By default, the source IP address of IGMP group-specific queries is 0.0.0.0.

This command takes effect only if IGMP snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**.

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
```

igmp-snooping static-group

Syntax

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

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

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

group-address: Specifies the address of the multicast group that the port joins as a static member port, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Specifies the address of the multicast source that the port joins as a static member port. The value of this argument should be a valid unicast address or 0.0.0.0. A source IP address of 0.0.0.0 means no restriction on the multicast source.

vlan *vlan-id*: Specifies the VLAN that comprises the ports, where *vlan-id* is in the range of 1 to 4094.

Description

Use **igmp-snooping static-group** to configure the static (*, G) or (S, G) entry for the port, namely, to configure the port as a static member port of the specified multicast group or source-group.

Use **undo igmp-snooping static-group** to restore the default.

By default, no ports are static member ports.

The **source-ip** *source-address* option in the command is meaningful only for IGMPv3 snooping. If IGMPv2 snooping is running, the **source-ip** *source-address* option does not take effect although you can include **source-ip** *source-address* in the command.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN.

In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Examples

```
# Configure GigabitEthernet 1/0/1 in VLAN 2 to be a static member port for (1.1.1.1, 232.1.1.1).
<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 232.1.1.1 source-ip 1.1.1.1
vlan 2
```

igmp-snooping static-router-port

Syntax

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

undo igmp-snooping static-router-port **vlan** *vlan-id*

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-id*: Specifies a VLAN, where *vlan-id* is in the range of 1 to 4094.

Description

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

Use **undo igmp-snooping static-router-port** to restore the default.

By default, no ports are static router ports.

This command takes effect in IGMP snooping-enabled VLANs.

This command does not take effect in a sub-VLAN of a multicast VLAN.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN.

In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Related commands: **subvlan**.

Examples

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

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

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-router-port vlan 2
```

igmp-snooping version

Syntax

igmp-snooping version *version-number*

undo igmp-snooping version

View

VLAN view

Default level

2: System level

Parameters

version-number: Specifies an IGMP snooping version, in the range of 2 to 3.

Description

Use **igmp-snooping version** to configure the IGMP snooping version.

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

By default, the IGMPv2 snooping is used.

This command can take effect only if IGMP snooping is enabled in the VLAN.

This command does not take effect in a sub-VLAN of a multicast VLAN.

Related commands: **igmp-snooping enable** and **subvlan**.

Examples

Enable IGMP snooping in VLAN 2, and specify IGMPv3 snooping.

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

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

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

```
[Sysname] vlan 2
```

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

```
[Sysname-vlan2] igmp-snooping version 3
```

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

Syntax

last-member-query-interval *interval*
undo last-member-query-interval

View

IGMP-snooping view

Default level

2: System level

Parameters

interval: Specifies the IGMP last-member query interval in seconds. The value ranges from 1 to 5.

Description

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

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

By default, the IGMP last-member query interval is 1 second.

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

This command takes effect only in IGMP snooping-enabled VLANs.

Related commands: **igmp-snooping last-member-query-interval**.

Examples

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

mac-address multicast

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 Ethernet interface view or Layer 2 aggregate interface view:

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

In port group view:

mac-address multicast *mac-address* **vlan** *vlan-id*
undo mac-address multicast *mac-address* **vlan** *vlan-id*

View

System view, Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

mac-address: Specifies a static multicast MAC address, which can be any multicast MAC address except 0100-5Exx-xxxx and 3333-xxxx-xxxx, where x represents an arbitrary hexadecimal number from 0 to F. A multicast MAC address is a MAC address whose the least significant bit of the most significant octet is 1. The system gives a prompt if the configured static multicast MAC address conflicts with the MAC address of other protocols.

interface-list: Specifies a list of interfaces. You can specify up to **n** single interfaces, interface ranges, or combinations of both for the list. A single interface takes the form of *interface-type interface-number*. An interface range takes the form of *interface-type interface-number to interface-type interface-number*, where the end interface number must be greater than the start interface number.

vlan vlan-id: Specifies the VLAN to which the interface belongs. *vlan-id* is in the range of 1 to 4094. The specified VLAN must exist and the system gives a prompt if the specified interface does not belong to the VLAN.

Description

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.

By default, no static multicast MAC address entry is configured.

If **multicast** is not specified when using the **undo mac-address multicast** command, all MAC address entries (including static multicast MAC address entries and unicast MAC address entries) are deleted.

Related commands: **display mac-address multicast**; **mac-address** (*Layer 2—LAN Switching Command Reference*).

Examples

Configure a static multicast MAC address entry with the MAC address of 0100-0001-0001 and outgoing interfaces 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 with the MAC address of 0100-0001-0001 in interface view of GigabitEthernet 1/0/1 in VLAN 2.

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

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-address multicast 0100-0001-0001 vlan 2
```

max-response-time (IGMP-snooping view)

Syntax

max-response-time *interval*

undo max-response-time

View

IGMP-snooping view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for IGMP general queries in seconds. The value ranges from 1 to 25.

Description

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

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

This command takes effect only in IGMP snooping-enabled VLANs.

Related commands: **igmp-snooping max-response-time** and **igmp-snooping query-interval**.

Examples

Set the maximum response delay for IGMP general queries globally to 5 seconds.

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

overflow-replace (IGMP-snooping view)

Syntax

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

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

View

IGMP-snooping view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command takes effect for all VLANs. If you specify one or more VLANs, the command takes effect for the specified VLANs only.

Description

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

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

By default, the multicast group replacement function is disabled.

This command takes effect in IGMP snooping-enabled VLANs.

Related commands: **igmp-snooping overflow-replace**.

Examples

Enable the multicast group replacement function globally in VLAN 2.

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

```
[Sysname] igmp-snooping
[Sysname-igmp-snooping] overflow-replace vlan 2
```

report-aggregation (IGMP-snooping view)

Syntax

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

View

IGMP-snooping view

Default level

2: System level

Parameters

None

Description

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

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

By default, IGMP report suppression is enabled.

This command takes effect in IGMP snooping-enabled VLANs.

Examples

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

reset igmp-snooping group

Syntax

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

View

User view

Default level

2: System level

Parameters

group-address: Specifies an IGMP snooping group. The value range of *group-address* is 224.0.1.0 to 239.255.255.255.

all: Specifies all IGMP snooping groups.

vlan *vlan-id*: Specifies a VLAN. The value range of *vlan-id* is 1 to 4094.

Description

Use **reset igmp-snooping group** to remove the dynamic group entries of the specified IGMP snooping groups.

This command takes effect only in IGMP snooping-enabled VLANs.

This command cannot remove the static group entries of IGMP snooping groups.

Examples

Remove the dynamic group entries of all IGMP snooping groups.

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

reset igmp-snooping statistics

Syntax

reset igmp-snooping statistics

View

User view

Default level

2: System level

Parameters

None

Description

Use **reset igmp-snooping statistics** to clear statistics for the IGMP messages learned by IGMP snooping.

Examples

Clear statistics for the IGMP messages learned by IGMP snooping.

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

router-aging-time (IGMP-snooping view)

Syntax

router-aging-time *interval*

undo router-aging-time

View

IGMP-snooping view

Default level

2: System level

Parameters

interval: Specifies an aging timer in seconds for dynamic router ports. The value ranges from 1 to 1000.

Description

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

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

By default, the aging timer of a dynamic router port is 105 seconds.

This command takes effect only in IGMP snooping-enabled VLANs.

Related commands: **igmp-snooping router-aging-time**.

Examples

Set the aging timer for dynamic router ports to 100 seconds globally.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] router-aging-time 100
```

source-deny (IGMP-snooping view)

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

View

IGMP-snooping view

Default level

2: System level

Parameters

interface-list: Specifies one or multiple ports. You can provide up to 10 port lists. For each list, you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number to interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

Description

Use **source-deny** to enable multicast source port filtering so that all multicast data packets are blocked.

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

By default, multicast source port filtering is not enabled.

This command takes effect in IGMP snooping-enabled VLANs.

Examples

Enable source port filtering for multicast data on interfaces 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
```

PIM snooping configuration commands

display pim-snooping neighbor

Syntax

display pim-snooping neighbor [**vlan** *vlan-id*] [**slot** *slot-number*] [[**{ begin | exclude | include }**] *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the PIM snooping neighbor information of the specified VLAN. The *vlan-id* argument is in the range of 1 to 4094. If no VLAN is specified, this command displays the PIM snooping neighbor information of all VLANs.

slot *slot-number*: Displays the PIM snooping neighbor information of the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

[**:**]: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

Examples

Display information about PIM snooping neighbors in VLAN 2.

```
<Sysname> display pim-snooping neighbor vlan 2
```

```
Total number of neighbors: 2
```

```
VLAN ID: 2
```

```
Total number of neighbors: 2
```

Neighbor	Port	Expires	Option Flags
10.1.1.2	GE1/0/1	02:02:23	LAN Prune Delay(T)
20.1.1.2	GE1/0/2	03:00:05	LAN Prune Delay

Table 5 Command output

Field	Description
Total number of neighbors	Total number of PIM snooping neighbors.
Neighbor	IP address of the PIM snooping neighbor.
Port	Name of the port that connects to the PIM snooping neighbor.
Expires	Remaining time before the PIM snooping neighbor expires. <i>Never</i> means the PIM snooping neighbor never expires.
Option Flags	<p>Possible values includes the following items:</p> <ul style="list-style-type: none"> • LAN Prune Delay—Indicates that the PIM hello messages received from the neighbor carry the LAN_Prune_Delay option. • LAN Prune Delay(T)—Indicates that the PIM hello messages received from the neighbor carry the LAN_Prune_Delay option, and the join suppression function has been disabled

display pim-snooping routing-table

Syntax

display pim-snooping routing-table [**vlan** *vlan-id*] [**slot** *slot-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the PIM snooping routing entries of the specified VLAN. The *vlan-id* argument is in the range of 1 to 4094. If no VLAN is specified, this command displays the PIM snooping routing entries in all VLANs.

slot *slot-number*: Displays the PIM snooping routing entries on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

Examples

Display the PIM snooping routing entries of VLAN 2.

```

<Sysname> display pim-snooping routing-table vlan 2 slot 1
  Total 1 entry(ies)
  FSM Flag: NI-no info, J-join, PP-prune pending

VLAN ID: 2
  Total 2 entry(ies)
  (172.10.10.1, 225.1.1.1)
    Upstream neighbor: 20.1.1.1
    Upstream port: GE1/0/1
    Total number of downstream ports: 1
      1: GE1/0/3
        Expires: 00:03:01, FSM: J
    Upstream neighbor: 10.1.1.1
    Upstream port: GE1/0/2
    Total number of downstream ports: 1
      1: GE1/0/4
        Expires: 00:01:05, FSM: J

```

Table 6 Command output

Field	Description
Total 1 entry(ies)	Total number of (S, G) entries and (*, G) entries in the PIM snooping routing table
FSM Flag: NI-no info, J-join, PP-prune pending	State machine flag of the downstream port. Possible values include: <ul style="list-style-type: none"> • NI—Initial state • J—Join • PP—Prune pending
(172.10.10.1, 225.1.1.1)	(S, G) entry
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry
Upstream port	Upstream port of the (S, G) entry or (*, G) entry)
Expires	Expiration time of the downstream port
FSM	State machine flag of the downstream port

display pim-snooping statistics

Syntax

```
display pim-snooping statistics [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

Examples

Display statistics for the PIM messages learned by 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 7 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

pim-snooping enable

Syntax

pim-snooping enable

undo pim-snooping enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

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

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

By default, PIM snooping is disabled.

Before you enable PIM snooping in a VLAN, be sure to enable IGMP snooping globally and specifically in the VLAN.

PIM snooping does not work in a sub-VLAN of a multicast VLAN.

Related commands: **igmp-snooping enable**.

Examples

Enable IGMP snooping globally, and enable IGMP snooping and PIM snooping in 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
```

reset pim-snooping statistics

Syntax

reset pim-snooping statistics

View

User view

Default level

2: System level

Parameters

None

Description

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

Examples

Clear statistics for the PIM messages learned by PIM snooping.

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

Multicast VLAN configuration commands

display multicast-vlan

Syntax

display multicast-vlan [*vlan-id*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan-id: Specifies a multicast VLAN, in the range of 1 to 4094. If this argument is not specified, this command displays information about all multicast VLANs.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display multicast-vlan** to display information about the specified multicast VLAN.

Examples

Display information about all multicast VLANs.

```
<Sysname> display multicast-vlan
Total 2 multicast-vlan(s)
```

```
Multicast vlan 100
  subvlan list:
    vlan 2  4-6
  port list:
    no port
```

```
Multicast vlan 200
  subvlan list:
    no subvlan
  port list:
    GE1/0/1          GE1/0/2
```

Table 8 Command output

Field	Description
subvlan list	List of sub-VLANs of the multicast VLAN
port list	Port list of the multicast VLAN

multicast-vlan

Syntax

multicast-vlan *vlan-id*

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

View

System view

Default level

2: System level

Parameters

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

all: Specifies all multicast VLANs.

Description

Use **multicast-vlan** to configure the specified VLAN as a multicast VLAN and enter multicast VLAN view.

Use **undo multicast-vlan** to remove the specified VLAN as a multicast VLAN.

The VLAN to be configured is not a multicast VLAN by default.

The specified VLAN to be configured as a multicast VLAN must exist.

For a sub-VLAN-based multicast VLAN, you must enable IGMP snooping only in the multicast VLAN. For a port-based multicast VLAN, you must enable IGMP snooping in both the multicast VLAN and all the user VLANs.

Related commands: **igmp-snooping enable**.

Examples

Enable IGMP snooping in VLAN 100. Configure it as a multicast VLAN and enter multicast VLAN 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]
```


port (multicast VLAN view)

Syntax

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

View

Multicast VLAN view

Default level

2: System level

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number* to *interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

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

Description

Use **port** to assign the specified ports to the current multicast VLAN.

Use **undo port** to delete the specified ports or all ports from the current multicast VLAN.

By default, a multicast VLAN has no ports.

A port can belong to only one multicast VLAN.

You can assign only Ethernet ports, and Layer 2 aggregate interfaces as multicast VLAN ports.

Examples

```
# Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to multicast VLAN 100.  
<Sysname> system-view  
[Sysname] multicast-vlan 100  
[Sysname-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

port multicast-vlan

Syntax

```
port multicast-vlan vlan-id  
undo port multicast-vlan
```

View

Ethernet interface view, Layer 2 aggregate interface view, port group view.

Default level

2: System level

Parameters

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

Description

Use **port multicast-vlan** to assign the current port to the specified multicast VLAN.

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

By default, a port does not belong to any multicast VLAN.

A port can belong to only one multicast VLAN.

Examples

Assign GigabitEthernet 1/0/1 to multicast VLAN 100.

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

subvlan (multicast VLAN view)

Syntax

subvlan *vlan-list*

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

View

Multicast VLAN view

Default level

2: System level

Parameters

vlan-list: Specifies a VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

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

Description

Use **subvlan** to configure sub-VLANs for the current multicast VLAN.

Use **undo subvlan** to remove the specified sub-VLANs or all sub-VLANs from the current multicast VLAN.

A multicast VLAN has no sub-VLANs by default.

The VLANs to be configured as sub-VLANs of the multicast VLAN must have existed and must not be multicast VLANs or sub-VLANs of another multicast VLAN.

The number of sub-VLANs of the multicast VLAN must not exceed the system-defined limit.

Examples

Configure VLAN 10 through VLAN 15 as sub-VLANs of multicast VLAN 100.

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

MLD snooping configuration commands

display mld-snooping group

Syntax

```
display mld-snooping group [ vlan vlan-id ] [ slot slot-number ] [ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the MLD snooping group information in the specified VLAN, where *vlan-id* is in the range of 1 to 4094. If you do not specify a VLAN, this command displays MLD snooping group information in all VLANs.

slot *slot-number*: Displays information about MLD snooping multicast groups on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

verbose: Displays the detailed MLD snooping group information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mld-snooping group** to display MLD snooping group information, including both dynamic and static MLD snooping group entries.

Examples

Display detailed MLD snooping group information in VLAN 2.

```
<Sysname> display mld-snooping group vlan 2 verbose
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port
```

```
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):2.
```

```

Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port(s).
    GE1/0/1                (D) ( 00:01:30 )
IP group(s):the following ip group(s) match to one mac group.
IP group address:FF1E::101
    (::, FF1E::101):
        Attribute:      Host Port
        Host port(s):total 1 port(s).
            GE1/0/2                (D) ( 00:03:23 )
MAC group(s):
MAC group address:3333-0000-0101
Host port(s):total 1 port(s).
    GE1/0/2

```

Table 9 Command output

Field	Description
Total 1 IP Group(s).	Total number of IPv6 multicast groups.
Total 1 IP Source(s).	Total number of IPv6 multicast sources.
Total 1 MAC Group(s).	Total number of MAC multicast groups.
Port flags: D-Dynamic port, S-Static port, C-Copy port, P-PIM port	Port flags: D —Dynamic port. S —Static port. C —Port copied from a (*, G) entry to an (S, G) entry. P —Port that IPv6 PIM snooping adds.
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R —Real egress sub-VLAN under the current entry. C —Sub-VLAN copied from a (*, G) entry to an (S, G) entry.
Router port(s)	Number of router ports.
(00:01:30)	Remaining time of the aging timer for the dynamic member port or router port.
IP group address	Address of IPv6 multicast group.
::, FF1E::101)	(S, G) entry, double colon represents all the multicast sources.
MAC group address	Address of MAC multicast group.
Attribute	Attribute of IPv6 multicast group.
Host port(s)	Number of member ports.

display mld-snooping host

Syntax

```

display mld-snooping host vlan vlan-id group ipv6-group-address [ source ipv6-source-address ] [ slot slot-number ] [ [ begin | exclude | include } regular-expression ]

```

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays information about the hosts tracked by MLD snooping in the specified VLAN, where *vlan-id* is in the range of 1 to 4094.

group *ipv6-group-address*: Displays information about the hosts tracked by MLD snooping that are in the specified IPv6 multicast group. The value of *ipv6-group-address* is in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

source *ipv6-source-address*: Displays information about the hosts tracked by MLD snooping that are in the specified IPv6 multicast source.

slot *slot-number*: Displays information about the hosts tracked by MLD snooping on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mld-snooping host** to display information about the hosts tracked by MLD snooping.

Examples

Display information about the hosts tracked by MLD snooping in multicast group FF1E::101 in VLAN 2.

```
<Sysname> display mld-snooping host vlan 2 group ff1e::101
```

```
VLAN(ID) : 2
```

```
(::, FF1E::101)
```

```
Port : GigabitEthernet1/0/1
```

Host	Uptime	Expires
1::1	00:02:20	00:00:40
2::2	00:02:21	00:00:39

```
Port : GigabitEthernet1/0/2
```

Host	Uptime	Expires
3::3	00:02:20	00:00:40

Table 10 Command output

Field	Description
(::, FF1E::101)	(S, G) entry, where :: indicates all IPv6 multicast sources
Port	Member port

Field	Description
Host	Host IPv6 address
Uptime	Host running duration
Expires	Host expiration time, where <i>timeout</i> means that the host has expired

display mld-snooping statistics

Syntax

display mld-snooping statistics [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mld-snooping statistics** to display statistics for the MLD messages learned through MLD snooping.

Examples

Display statistics for the MLD 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 error MLD messages:0.
```

Table 11 Command output

Field	Description
general queries	General query messages
specific queries	Multicast-address-specific query messages
reports	Report messages
done	Done messages
reports with right and wrong records	Reports that contain correct and incorrect records
specific sg queries	Multicast-address-and-source-specific queries

dot1p-priority (MLD-snooping view)

Syntax

dot1p-priority *priority-number*

undo dot1p-priority

View

MLD-snooping view

Default level

2: System level

Parameters

priority-number: Specifies an 802.1p precedence for MLD messages, in the range of 0 to 7. A higher number indicates a higher precedence.

Description

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

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

The default 802.1p precedence for MLD messages is 0.

Examples

Set the 802.1p precedence for MLD messages to 3 globally.

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

```
[Sysname] mld-snooping
```

```
[Sysname-mld-snooping] dot1p-priority 3
```

dscp (MLD-snooping view)

Syntax

dscp *dscp-value*

undo dscp

View

MLD-snooping view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value for MLD messages, in the range of 0 to 63.

Description

Use **dscp** to set the DSCP value for MLD messages.

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

The default DSCP value in MLD messages is 48.

This command applies to only the MLD messages that the local switch generates when the switch or its port acts as a member host, rather than those forwarded ones.

Examples

Set the DSCP value to 63 for MLD messages.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] dscp 63
```

fast-leave (MLD-snooping view)

Syntax

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

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

View

MLD-snooping view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command applies to all VLANs. If you specify one or multiple VLANs, the command applies to the specified VLANs only.

Description

Use **fast-leave** to enable fast-leave processing globally. With this function enabled, when the switch receives an MLD done message on a port, it directly removes that port from the forwarding table entry for the specific group.

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

By default, fast-leave processing is disabled.

This command takes effect in MLD snooping-enabled VLANs.

Related commands: **mld-snooping fast-leave**.

Examples

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

group-policy (MLD-snooping view)

Syntax

```
group-policy acl6-number [ vlan vlan-list ]
undo group-policy [ vlan vlan-list ]
```

View

MLD-snooping view

Default level

2: System level

Parameters

acl6-number: Specifies a basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced IPv6 ACL rule matches the IPv6 multicast source address or addresses specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX or TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command applies to all VLANs. If you specify one or multiple VLANs, the command applies to the specified VLANs only.

Description

Use **group-policy** to configure a global IPv6 multicast group filter, namely, to control the IPv6 multicast groups that a host can join.

Use **undo group-policy** to remove the configured global IPv6 multicast group filter.

By default, no IPv6 multicast group filter is configured globally. Namely, any host can join any valid IPv6 multicast group.

If the specified IPv6 ACL does not exist or the ACL rule is null, all IPv6 multicast groups are filtered out.

You can configure different IPv6 ACL rules for each port in different VLANs. For a given VLAN, a newly configured IPv6 ACL rule overrides the existing one.

Related commands: **mld-snooping group-policy**.

Examples

```
# Apply ACL 2000 as an IPv6 multicast group filter so that hosts in VLAN 2 can join FF03::101 only.
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff03::101 16
[Sysname-acl6-basic-2000] quit
[Sysname] mld-snooping
```

```
[Sysname-mld-snooping] group-policy 2000 vlan 2
```

host-aging-time (MLD-snooping view)

Syntax

host-aging-time *interval*

undo host-aging-time

View

MLD-snooping view

Default level

2: System level

Parameters

interval: Specifies an aging timer for dynamic member ports in seconds. The value range is 200 to 1000.

Description

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

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

By default, the aging timer of a dynamic member port is 260 seconds.

This command takes effect only in MLD snooping-enabled VLANs.

Related commands: **mld-snooping host-aging-time**.

Examples

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

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

host-tracking (MLD-snooping view)

Syntax

host-tracking

undo host-tracking

View

MLD-snooping view

Default level

2: System level

Parameters

None

Description

Use **host-tracking** to enable the MLD snooping host tracking function globally.

Use **undo host-tracking** to disable the MLD snooping host tracking function globally.

By default, this function is disabled.

This command takes effect only in MLD snooping-enabled VLANs.

Related commands: **display mld-snooping host** and **mld-snooping host-tracking**.

Examples

```
# Enable the MLD snooping host tracking function globally.
```

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

```
[Sysname] mld-snooping
```

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

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

Syntax

last-listener-query-interval *interval*

undo last-listener-query-interval

View

MLD-snooping view

Default level

2: System level

Parameters

interval: Sets the MLD last-listener query interval in seconds. The value range is 1 to 5.

Description

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

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

By default, the MLD last-listener query interval is 1 second.

The MLD last-listener query interval determines the interval for sending MLD multicast-address-specific queries and the maximum response delay for MLD multicast-address-specific queries.

This command takes effect only in MLD snooping-enabled VLANs.

Related commands: **mld-snooping last-listener-query-interval**.

Examples

```
# Set the MLD last listener query interval to 3 seconds globally.
```

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

```
[Sysname] mld-snooping
```

```
[Sysname-mld-snooping] last-listener-query-interval 3
```

max-response-time (MLD-snooping view)

Syntax

max-response-time *interval*

undo max-response-time

View

MLD-snooping view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for MLD general queries in seconds. The value ranges from 1 to 25.

Description

Use **max-response-time** to configure the maximum response time for MLD general queries globally.

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

By default, the maximum response delay for MLD general queries is 10 seconds.

This command takes effect only in MLD snooping-enabled VLANs.

Related commands: **mld-snooping max-response-time** and **mld-snooping query-interval**.

Examples

Set the maximum response delay for MLD general queries to 5 seconds globally.

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

mld-snooping

Syntax

mld-snooping

undo mld-snooping

View

System view

Default level

2: System level

Parameters

None

Description

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

Use **undo mld-snooping** to disable MLD snooping globally.

By default, MLD snooping is disabled.

Related commands: **mld-snooping enable**.

Examples

Enable MLD snooping globally and enter MLD-snooping view.

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

mld-snooping access-policy

Syntax

```
mld-snooping access-policy acl6-number  
undo mld-snooping access-policy { acl6-number | all }
```

View

User profile view

Default level

2: System level

Parameters

acl6-number: Specifies a basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL matches the multicast source address or addresses specified in MLDv2 reports, rather than the source address in the IP packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX and TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

all: Specifies all IPv6 ACLs.

Description

Use **mld-snooping access-policy** to configure an IPv6 multicast user control policy.

Use **undo mld-snooping access-policy** to remove the configuration.

By default, no IPv6 user control policy is configured. Namely, a user can join any valid IPv6 multicast group.

You can use this command repeatedly to configure multiple IPv6 multicast user control policies.

Examples

Create and enable a user profile named **abc**, and configure the user profile so that users in this user profile can join FF03::101 only.

```
<Sysname> system-view  
[Sysname] acl ipv6 number 2001  
[Sysname-acl6-basic-2001] rule permit source ff03::101 16  
[Sysname-acl6-basic-2001] quit  
[Sysname] user-profile abc  
[Sysname-user-profile-abc] mld-snooping access-policy 2001  
[Sysname-user-profile-abc] quit  
[Sysname] user-profile abc enable
```

mld-snooping done source-ip

Syntax

```
mld-snooping done source-ip { ipv6-address | current-interface }  
undo mld-snooping done source-ip
```

View

VLAN view

Default level

2: System level

Parameters

ipv6-address: Specifies a source IPv6 address for the MLD done messages that the MLD snooping proxy sends, which can be any legal IPv6 link-local address.

current-interface: Specifies the IPv6 link-local address of the current VLAN interface as the source address of MLD done messages that the MLD snooping proxy sends. If no IPv6 address has been assigned to the current interface, the default IPv6 address FE80::02FF:FFFF:FE00:0001 is used.

Description

Use **mld-snooping done source-ip** to configure the source IPv6 address of the MLD done messages that the MLD snooping proxy sends.

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

By default, the source IPv6 address of the MLD done messages that the MLD snooping proxy sends is FE80::02FF:FFFF:FE00:0001.

Before you configure this command in a VLAN, enable MLD snooping for the VLAN.

The source IPv6 address configured in the **mld-snooping done source-ip** command also applies when the simulated host sends MLD done messages.

Related commands: **mld-snooping enable**.

Examples

Enable MLD snooping in VLAN 2 and configure the source IPv6 address of MLD done messages that the MLD snooping proxy sends in VLAN 2 to FE80:0:0:1::1.

```
<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
```

mld-snooping dot1p-priority

Syntax

mld-snooping dot1p-priority *priority-number*

undo mld-snooping dot1p-priority

View

VLAN view

Default level

2: System level

Parameters

priority-number: Specifies an 802.1p precedence for MLD messages, in the range of 0 to 7. A higher number indicates a higher precedence.

Description

Use **mld-snooping dot1p-priority** to set the 802.1p precedence for the MLD messages in a VLAN.

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

The default 802.1p precedence for the MLD messages in a VLAN is 0.

Before you configure this command in a VLAN, enable MLD snooping for the VLAN.

Related commands: **mld-snooping enable**.

Examples

Enable MLD snooping in VLAN 2 and set the 802.1p precedence for the MLD messages in the VLAN 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
```

mld-snooping drop-unknown

Syntax

mld-snooping drop-unknown

undo mld-snooping drop-unknown

View

VLAN view

Default level

2: System level

Parameters

None

Description

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

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

By default, this function is disabled, and unknown IPv6 multicast data is flooded in the VLAN.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **mld-snooping enable**.

Examples

Enable MLD snooping and the function for dropping unknown IPv6 multicast data in VLAN 2.

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

```
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping drop-unknown
```

mld-snooping enable

Syntax

mld-snooping enable
undo mld-snooping enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

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

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

By default, MLD snooping is disabled in a VLAN.

MLD snooping must be enabled globally before it can be enabled in a VLAN

Related commands: **mld-snooping**.

Examples

```
# Enable MLD snooping in VLAN 2.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
```

mld-snooping fast-leave

Syntax

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

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **mld-snooping fast-leave** to enable fast-leave processing on the current port or group of ports. With this function enabled, when the switch receives an MLD done message on a port, it directly removes that port from the forwarding table entry for the specific group.

Use **undo mld-snooping fast-leave** to disable fast-leave processing on the current port or group of ports. By default, fast-leave processing is disabled.

This command takes effect in MLD snooping-enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **fast-leave**.

Examples

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

mld-snooping general-query source-ip

Syntax

mld-snooping general-query source-ip { *ipv6-address* | **current-interface** }
undo mld-snooping general-query source-ip

View

VLAN view

Default level

2: System level

Parameters

ipv6-address: Specifies the source IPv6 address of MLD general queries, which can be any legal IPv6 link-local address.

current-interface: Sets the source IPv6 link-local address of MLD general queries to the IPv6 address of the current VLAN interface. If the current VLAN interface does not have an IPv6 address, the default IPv6 address FE80::02FF:FFFF:FE00:0001 is used as the source IPv6 address of MLD general queries.

Description

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

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

By default, the source IPv6 address of MLD general queries is FE80::02FF:FFFF:FE00:0001.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **mld-snooping enable**.

Examples

In VLAN 2, enable MLD snooping and specify FE80:0:0:1::1 as the source IPv6 address of 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
```

mld-snooping group-limit

Syntax

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

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

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

limit: Specifies the maximum number of IPv6 multicast groups that a port can join. The value ranges from 1 to 1000.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

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

Use **undo mld-snooping group-limit** to restore the default.

By default, the upper limit is 1000.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Examples

```
# Configure to allow up to 10 IPv6 multicast groups that GigabitEthernet 1/0/1 in VLAN 2 can join.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping group-limit 10 vlan 2
```

mld-snooping group-policy

Syntax

mld-snooping group-policy *acl6-number* [**vlan** *vlan-list*]

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

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

acl6-number: Specifies a basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The IPv6 source address or address range specified in the advanced IPv6 ACL rule is the IPv6 multicast source addresses specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX or TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

Use **mld-snooping group-policy** to configure an IPv6 multicast group filter on the current ports, namely, to control the multicast groups that the hosts on the port can join.

Use **undo mld-snooping group-policy** to remove the configured IPv6 multicast group filter on the current port or ports.

By default, no IPv6 multicast group filter is configured on a port. Namely, a host can join any valid IPv6 multicast group.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

If the specified ACL does not exist or the ACL rule is null, all IPv6 multicast groups are filtered out.

You can configure different IPv6 ACL rules for each port in different VLANs. For a given VLAN, a newly configured IPv6 ACL rule overrides the existing one.

Related commands: **group-policy**.

Examples

Apply ACL 2000 as an IPv6 multicast group filter so that hosts on GigabitEthernet 1/0/1 in VLAN 2 can join FF03::101 only.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff03::101 16
[Sysname-acl6-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping group-policy 2000 vlan 2
```

mld-snooping host-aging-time

Syntax

mld-snooping host-aging-time *interval*

undo mld-snooping host-aging-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an aging timer for dynamic member ports in seconds. The value range is 200 to 1000.

Description

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

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

By default, the aging timer of a dynamic member port is 260 seconds.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **display mld-snooping host**, **host-aging-time** and **mld-snooping enable**.

Examples

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

```
<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
```

mld-snooping host-join

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*

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

ipv6-group-address: Specifies the address of the IPv6 multicast group that the simulated host will join. The value ranges from FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive.

ipv6-source-address: Specifies the address of the IPv6 multicast source that the simulated host will join.

vlan *vlan-id*: Specifies a VLAN that comprises the port or ports, where *vlan-id* is in the range of 1 to 4094.

Description

Use **mld-snooping host-join** to enable simulated joining on a port. Namely, you configure a port as a simulated member host for the specified IPv6 multicast group or source and group.

Use **undo mld-snooping host-join** to remove the simulated member host from the specified IPv6 multicast group or source and group.

By default, this function is disabled.

This command takes effect in MLD snooping-enabled VLANs. The version of MLD on the simulated member host is consistent with the version of MLD snooping that runs in the VLAN.

The **source-ip** *ipv6-source-address* option in the command is meaningful only for MLDv2 snooping. If MLDv1 snooping is running, the **source-ip** *ipv6-source-address* option does not take effect although you can include **source-ip** *ipv6-source-address* in the command.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN. In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Examples

Configure GigabitEthernet 1/0/1 in VLAN 2 to join (2002::22, FF3E::101) as a simulated host.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping host-join ff3e::101 source-ip 2002::22 vlan
2
```

mld-snooping host-tracking

Syntax

mld-snooping host-tracking
undo mld-snooping host-tracking

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping host-tracking** to enable the MLD snooping host tracking function in a VLAN.

Use **undo mld-snooping host-tracking** to disable the MLD snooping host tracking function in a VLAN.

By default, this function is disabled.

Before you configure this command, enable MLD snooping for the VLAN first.

Related commands: **host-tracking**, and **mld-snooping enable**.

Examples

```
# Enable MLD snooping and the MLD snooping host tracking function for VLAN 2.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping host-tracking
```

mld-snooping last-listener-query-interval

Syntax

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

View

VLAN view

Default level

2: System level

Parameters

interval: Sets the MLD last-listener query interval in seconds. The value ranges from 1 to 5.

Description

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.

By default, the MLD last listener query interval is 1 second.

The MLD last-listener query interval determines the interval for sending MLD multicast-address-specific queries and the maximum response delay for MLD multicast-address-specific queries in a VLAN.

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

Related commands: **last-listener-query-interval** and **mld-snooping enable**.

Examples

Enable MLD snooping and set the MLD last listener query interval to 3 seconds in VLAN 2.

```
<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
```

mld-snooping max-response-time

Syntax

mld-snooping max-response-time *interval*

undo mld-snooping max-response-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies the maximum response delay for MLD general queries in seconds. The value ranges from 1 to 25.

Description

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

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

By default, the maximum response delay for MLD general queries is 10 seconds.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **max-response-time**, **mld-snooping enable**, and **mld-snooping query-interval**.

Examples

Enable MLD snooping and set the maximum response delay for MLD general queries to 5 seconds in VLAN 2.

```
<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
```

mld-snooping overflow-replace

Syntax

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

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

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

Use **undo mld-snooping overflow-replace** to disable the IPv6 multicast group replacement function.

By default, the IPv6 multicast group replacement function is disabled.

This command takes effect in MLD snooping-enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified VLANs.

Related commands: **overflow-replace**.

Examples

```
# Enable the IPv6 multicast group replacement function on GigabitEthernet 1/0/1 in VLAN 2.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping overflow-replace vlan 2
```

mld-snooping proxying enable

Syntax

```
mld-snooping proxying enable
undo mld-snooping proxying enable
```


View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping proxying enable** to enable the MLD snooping proxying function in a VLAN.

Use **undo mld-snooping proxying enable** to disable the MLD snooping proxying function in a VLAN.

By default, MLD snooping proxying is disabled in all VLANs.

Before you configure this command in a VLAN, enable MLD snooping for the VLAN.

Related commands: **mld-snooping enable**.

Examples

Enable MLD snooping and then MLD snooping proxying in VLAN 2.

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

mld-snooping querier

Syntax

mld-snooping querier

undo mld-snooping querier

View

VLAN view

Default level

2: System level

Parameters

None

Description

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

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

By default, the MLD snooping querier function is disabled.

This command takes effect only if MLD snooping is enabled for the VLAN, and it does not take effect in a sub-VLAN of an IPv6 multicast VLAN.

Related commands: **mld-snooping enable** and **subvlan**.

Examples

Enable MLD snooping and the MLD snooping querier function in VLAN 2.

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

mld-snooping query-interval

Syntax

mld-snooping query-interval *interval*
undo mld-snooping query-interval

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an MLD query interval in seconds, namely, the length of time that the device waits between sending MLD general queries. The value ranges from 2 to 300.

Description

Use **mld-snooping query-interval** to configure the MLD query interval.

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

By default, the MLD query interval is 125 seconds.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **max-response-time**, **mld-snooping enable**, **mld-snooping max-response-time**, and **mld-snooping querier**.

Examples

Enable MLD snooping and set the MLD query interval to 20 seconds in VLAN 2.

```
<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
```

mld-snooping report source-ip

Syntax

mld-snooping report source-ip { *ipv6-address* | **current-interface** }
undo mld-snooping report source-ip

View

VLAN view

Default level

2: System level

Parameters

ipv6-address: Specifies a source IPv6 address for the MLD reports that the MLD snooping proxy sends, which can be any legal IPv6 link-local address.

current-interface: Specifies the IPv6 link-local address of the current VLAN interface as the source address of MLD reports that the MLD snooping proxy sends. If no IPv6 address has been assigned to the current interface, the default IPv6 address FE80::02FF:FFFF:FE00:0001 is used.

Description

Use **mld-snooping report source-ip** to configure the source IPv6 address of the MLD reports that the MLD snooping proxy sends.

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

By default, the source IPv6 address of the MLD reports that the MLD snooping proxy sends is FE80::02FF:FFFF:FE00:0001.

Before you configure this command in a VLAN, enable MLD snooping for the VLAN.

The source IPv6 address configured in the **mld-snooping report source-ip** command also applies when the simulated host sends MLD reports.

Related commands: **mld-snooping enable**.

Examples

Enable MLD snooping in VLAN 2 and configure the source IPv6 address of MLD reports that the MLD snooping proxy sends in VLAN 2 to FE80:0:0:1::1.

```
<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
```

mld-snooping router-aging-time

Syntax

mld-snooping router-aging-time *interval*

undo mld-snooping router-aging-time

View

VLAN view

Default level

2: System level

Parameters

interval: Specifies an aging timer for dynamic router ports, in seconds. The value ranges from 1 to 1,000.

Description

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

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

By default, the aging timer of a dynamic router port is 260 seconds.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **mld-snooping enable** and **router-aging-time**.

Examples

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

```
<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
```

mld-snooping router-port-deny

Syntax

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

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

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

Description

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

Use **undo mld-snooping router-port-deny** to restore the default.

By default, a port can become a dynamic router port.

This command takes effect in MLD snooping-enabled VLANs.

If you do not specify any VLAN when using this command in Layer 2 Ethernet interface view or Layer 2 aggregate interface view, the command takes effect for all VLANs that the interface belongs to. If you specify one or multiple VLANs, the command takes effect for the specified VLANs that the interface belongs to.

If you do not specify any VLAN when using this command in port group view, the command takes effect on all the ports in this group. If you specify one or multiple VLANs, the command takes effect only on those ports in this group that belong to the specified 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

Syntax

mld-snooping source-deny
undo mld-snooping source-deny

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **mld-snooping source-deny** to enable IPv6 multicast source port filtering.

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

By default, IPv6 multicast source port filtering is disabled.

This command takes effect in MLD snooping-enabled VLANs.

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
```

mld-snooping special-query source-ip

Syntax

mld-snooping special-query source-ip { *ipv6-address* | **current-interface }**
undo mld-snooping special-query source-ip

View

VLAN view

Default level

2: System level

Parameters

ipv6-address: Specifies an IPv6 link-local address as the source IPv6 address of MLD multicast-address-specific queries.

current-interface: Specifies the source IPv6 link-local address of the VLAN interface of the current VLAN as the source IPv6 address of MLD multicast-address-specific queries. If the current VLAN interface does not have an IPv6 address, the default IPv6 address FE80::02FF:FFFF:FE00:0001 is used as the source IPv6 address of MLD multicast-address-specific queries.

Description

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

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

By default, the source IPv6 address of MLD multicast-address-specific queries is FE80::02FF:FFFF:FE00:0001.

This command takes effect only if MLD snooping is enabled for the VLAN.

Related commands: **mld-snooping enable**.

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
```

mld-snooping static-group

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*

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

ipv6-group-address: Specifies the address of the IPv6 multicast group that the port will join as a static member port. The value ranges from FFxy::/16—excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::, where x and y represent any hexadecimal number between 0 and F, inclusive.

ipv6-source-address: Specifies the address of the IPv6 multicast source that the port will join as a static member port.

vlan *vlan-id*: Specifies the VLAN that comprises the Ethernet ports, where *vlan-id* is in the range of 1 to 4094.

Description

Use **mld-snooping static-group** to configure the static IPv6 (*, G) or (S, G) joining function, that is, to configure the port as a static member port of an IPv6 multicast group or source and group.

Use **undo mld-snooping static-group** to restore the default.

By default, no ports are static member ports.

The **source-ip** *ipv6-source-address* option in the command is meaningful only for MLDv2 snooping. If MLDv1 snooping is running, the **source-ip** *ipv6-source-address* option does not take effect although you can include **source-ip** *ipv6-source-address* in the command.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN. In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Examples

```
# Configure GigabitEthernet 1/0/1 in VLAN 2 as a static member port for (2002::22, FF3E::101).
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping static-group ff3e::101 source-ip 2002::22
vlan 2
```

mld-snooping static-router-port

Syntax

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

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

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view, port group view

Default level

2: System level

Parameters

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

Description

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

Use **undo mld-snooping static-router-port** to restore the default.

By default, no ports are static router ports.

This command takes effect in MLD snooping-enabled VLANs.

This command does not take effect in a sub-VLAN of an IPv6 multicast VLAN.

In Layer 2 Ethernet interface view or Layer 2 aggregate interface view, this command takes effect only if the interface belongs to the specified VLAN. In port group view, this command takes effect only on those ports in this port group that belong to the specified VLAN.

Related commands: **subvlan**.

Examples

```
# Enable the static router port function on GigabitEthernet 1/0/1 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

Syntax

mld-snooping version *version-number*

undo mld-snooping version

View

VLAN view

Default level

2: System level

Parameters

version-number: Specifies an MLD snooping version. The value can be 1 or 2.

Description

Use **mld-snooping version** to configure the MLD snooping version.

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

By default, the MLDv1 snooping is used.

This command can take effect only if MLD snooping is enabled for the VLAN, and it does not take effect in a sub-VLAN of an IPv6 multicast VLAN.

Related commands: **mld-snooping enable** and **subvlan**.

Examples

```
# Enable MLD snooping in VLAN 2, and specify MLDv2 snooping.
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
```

overflow-replace (MLD-snooping view)

Syntax

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

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

View

MLD-snooping view

Default level

2: System level

Parameters

vlan *vlan-list*: Specifies one or multiple VLANs. You can provide up to 10 VLAN lists. For each list, you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id to end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094. If you do not specify any VLAN, the command applies to all VLANs. If you specify one or multiple VLANs, the command applies to the specified VLANs only.

Description

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

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

By default, the IPv6 multicast group replacement function is disabled globally.

This command takes effect in MLD snooping-enabled VLANs.

Related commands: **mld-snooping overflow-replace**.

Examples

Enable the IPv6 multicast group replacement function globally in VLAN 2.

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

report-aggregation (MLD-snooping view)

Syntax

report-aggregation

undo report-aggregation

View

MLD-snooping view

Default level

2: System level

Parameters

None

Description

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

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

By default, MLD report suppression is enabled.

This command takes effect in MLD snooping-enabled VLANs.

Examples

Disable MLD report suppression.

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

[Sysname-mld-snooping] undo report-aggregation

reset mld-snooping group

Syntax

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

View

User view

Default level

2: System level

Parameters

ipv6-group-address: Specifies an IPv6 multicast group. The value range of *ipv6-group-address* is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive.

all: Specifies all IPv6 multicast groups.

vlan *vlan-id*: Specifies a VLAN. The value range of *vlan-id* is 1 to 4094.

Description

Use **reset mld-snooping group** to remove the dynamic group entries of a specified MLD snooping group or all MLD snooping groups.

This command takes effect only in MLD snooping-enabled VLANs.

This command cannot remove the static group entries of MLD snooping groups.

Examples

Remove the dynamic group entries of all MLD snooping groups.

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

reset mld-snooping statistics

Syntax

reset mld-snooping statistics

View

User view

Default level

2: System level

Parameters

None

Description

Use **reset mld-snooping statistics** to clear statistics for the MLD messages learned by MLD snooping.

Examples

Clear statistics for the MLD messages learned by MLD snooping.

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

router-aging-time (MLD-snooping view)

Syntax

router-aging-time *interval*
undo router-aging-time

View

MLD-snooping view

Default level

2: System level

Parameters

interval: Specifies an aging timer in seconds for dynamic router ports. The value ranges from 1 to 1,000.

Description

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

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

By default, the aging time of a dynamic router port is 260 seconds.

This command takes effect only in MLD snooping-enabled VLANs.

Related commands: **mld-snooping router-aging-time**.

Examples

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

source-deny (MLD-snooping view)

Syntax

source-deny port *interface-list*
undo source-deny port *interface-list*

View

MLD-snooping view

Default level

2: System level

Parameters

interface-list: Specifies a list of ports. You can specify multiple ports or port ranges by providing the this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }, where *interface-type* is the port type and *interface-number* is the port number.

Description

Use **source-deny** to enable IPv6 multicast source port filtering, namely, to filter out all the received IPv6 multicast packets.

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

By default, IPv6 multicast source port filtering is disabled.

This command takes effect in MLD snooping-enabled VLANs.

Examples

Enable source port filtering for IPv6 multicast data on interfaces 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
```

IPv6 PIM snooping configuration commands

display pim-snooping ipv6 neighbor

Syntax

display pim-snooping ipv6 neighbor [**vlan** *vlan-id*] [**slot** *slot-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the IPv6 PIM snooping neighbor information of the specified VLAN. The *vlan-id* argument is in the range of 1 to 4094. If no VLAN is specified, this command displays the IPv6 PIM snooping neighbor information in all VLANs.

slot *slot-number*: Displays the IPv6 PIM snooping neighbor information on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

Examples

Display the IPv6 PIM snooping neighbor information of VLAN 2.

```
<Sysname> display pim-snooping ipv6 neighbor vlan 2
```

```
Total number of neighbors: 2
```

```
VLAN ID: 2
```

```
Total number of neighbors: 2
```

Neighbor	Port	Expires	Option Flags
FE80::6401:101	GE1/0/1	02:02:23	LAN Prune Delay(T)
FE80::C801:101	GE1/0/2	03:00:05	LAN Prune Delay

Table 12 Command output

Field	Description
Total number of neighbors	Total number of IPv6 PIM snooping neighbors.
Neighbor	IP address of the IPv6 PIM snooping neighbor.
Port	Name of the port that connects to the IPv6 PIM snooping neighbor.
Expires	Remaining time before the IPv6 PIM snooping neighbor expires. <i>Never</i> means the IPv6 PIM snooping neighbor never expires.
Option Flags	<p>Possible values includes the following items:</p> <ul style="list-style-type: none"> • LAN Prune Delay—Indicates that the IPv6 PIM hello messages received from the neighbor carry the LAN_Prune_Delay option. • LAN Prune Delay(T)—Indicates that the IPv6 PIM hello messages received from the neighbor carry the LAN_Prune_Delay option, and the join suppression function has been disabled.

display pim-snooping ipv6 routing-table

Syntax

display pim-snooping ipv6 routing-table [**vlan** *vlan-id*] [**slot** *slot-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the IPv6 PIM snooping routing entries of the specified VLAN. The *vlan-id* argument is in the range of 1 to 4094.

slot *slot-number*: Displays the IPv6 PIM snooping routing entries on the specified IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric. If no IRF fabric exists, the *slot-number* argument is the current device number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

Examples

```
# Display the IPv6 PIM snooping routing entries of VLAN 2.
<Sysname> display pim-snooping ipv6 routing-table vlan 2 slot 1
```

```

Total 1 entry(ies)
FSM Flag: NI-no info, J-join, PP-prune pending

VLAN ID: 2
  Total 2 entry(ies)
  (2000::1, FF1E::1)
    Upstream neighbor: FE80::101
    Upstream port: GE1/0/1
    Total number of downstream ports: 2
    1: GE1/0/3
      Expires: 00:03:01, FSM: J
    Upstream neighbor: FE80::102
    Upstream port: GE1/0/2
    Total number of downstream ports: 1
    1: GE1/0/4
      Expires: 00:01:05, FSM: J

```

Table 13 Command output

Field	Description
Total 1 entry(ies)	Total number of (S, G) entries and (*, G) entries in the IPv6 PIM snooping routing table.
FSM Flag: NI-no info, J-join, PP-prune pending	State machine flag of the downstream port. Possible values include: <ul style="list-style-type: none"> • NI—Initial state. • J—Join. • PP—Prune pending.
(2000::1, FF1E::1)	(S, G) entry.
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry.
Upstream port	Upstream port of the (S, G) entry or (*, G) entry).
Expires	Expiration time of the downstream port.
FSM	State machine of the downstream port.

display pim-snooping ipv6 statistics

Syntax

```
display pim-snooping ipv6 statistics [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

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

Examples

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

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

Table 14 Command output

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

pim-snooping ipv6 enable

Syntax

pim-snooping ipv6 enable

undo pim-snooping ipv6 enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

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

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

By default, IPv6 PIM snooping is disabled.

Before you enable IPv6 PIM snooping in a VLAN, be sure to enable MLD snooping globally and specially in the VLAN.

IPv6 PIM snooping does not work in a sub-VLAN of a multicast VLAN.

Related commands: **mld-snooping enable**.

Examples

Enable MLD snooping globally, and enable MLD snooping and IPv6 PIM snooping in VLAN 2.

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

reset pim-snooping ipv6 statistics

Syntax

reset pim-snooping ipv6 statistics

View

User view

Default level

2: System level

Parameters

None

Description

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

Examples

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

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

IPv6 multicast VLAN configuration commands

display multicast-vlan ipv6

Syntax

```
display multicast-vlan ipv6 [ vlan-id ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vlan-id: Specifies an IPv6 multicast VLAN, in the range of 1 to 4094. If this argument is not specified, this command displays information about all IPv6 multicast VLANs.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display multicast-vlan ipv6** to display information about the specified IPv6 multicast VLAN or all IPv6 multicast VLANs.

Examples

Display information about all IPv6 multicast VLANs.

```
<Sysname> display multicast-vlan ipv6
Total 2 IPv6 multicast-vlan(s)
```

```
IPv6 Multicast vlan 100
  subvlan list:
    vlan 2  4-6
  port list:
    no port
```

```
IPv6 Multicast vlan 200
  subvlan list:
    no subvlan
  port list:
    GE1/0/1          GE1/0/2
```

Table 15 Command output

Field	Description
subvlan list	List of sub-VLANs of the IPv6 multicast VLAN
port list	Port list of the IPv6 multicast VLAN

multicast-vlan ipv6

Syntax

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

View

System view

Default level

2: System level

Parameters

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

all: Specifies all IPv6 multicast VLANs.

Description

Use **multicast-vlan ipv6** to configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.

Use **undo multicast-vlan ipv6** to remove the specified VLAN as an IPv6 multicast VLAN.

No VLAN is an IPv6 multicast VLAN by default.

The specified VLAN to be configured as an IPv6 multicast VLAN must exist.

For a sub-VLAN-based IPv6 multicast VLAN, you must enable MLD snooping only in the IPv6 multicast VLAN. For a port-based IPv6 multicast VLAN, you must enable MLD snooping in both the IPv6 multicast VLAN and all the user VLANs.

Related commands: **mld-snooping enable**.

Examples

Enable MLD snooping in VLAN 100. Configure it as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 100
[Sysname-vlan100] mld-snooping enable
[Sysname-vlan100] quit
[Sysname] multicast-vlan ipv6 100
[Sysname-ipv6-mvlan-100]
```

port (IPv6 multicast VLAN view)

Syntax

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

View

IPv6 multicast VLAN view

Default level

2: System level

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number* to *interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

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

Description

Use **port** to assign the specified ports to the current IPv6 multicast VLAN.

Use **undo port** to delete the specified ports from the current IPv6 multicast VLAN.

By default, an IPv6 multicast VLAN has no ports.

A port can belong to only one IPv6 multicast VLAN.

You can assign only Ethernet ports, and Layer 2 aggregate interfaces to a multicast VLAN.

Examples

```
# Assign ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to IPv6 multicast VLAN 100.  
<Sysname> system-view  
[Sysname] multicast-vlan ipv6 100  
[Sysname-ipv6-mvlan-100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
```

port multicast-vlan ipv6

Syntax

```
port multicast-vlan ipv6 vlan-id  
undo port multicast-vlan ipv6
```

View

Ethernet interface view, Layer 2 aggregate interface view, port group view.

Default level

2: System level

Parameters

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

Description

Use **port multicast-vlan ipv6** to assign the current port to the specified IPv6 multicast VLAN.

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

By default, a port does not belong to any IPv6 multicast VLAN.

A port can belong to only one IPv6 multicast VLAN.

Examples

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

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

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port multicast-vlan ipv6 100
```

subvlan (IPv6 multicast VLAN view)

Syntax

subvlan *vlan-list*

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

View

IPv6 multicast VLAN view

Default level

2: System level

Parameters

vlan-list: Specifies a VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The value range of a VLAN ID is 1 to 4094.

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

Description

Use **subvlan** to configure sub-VLANs for the current IPv6 multicast VLAN.

Use **undo subvlan** to remove the specified sub-VLANs or all sub-VLANs from the current IPv6 multicast VLAN.

An IPv6 multicast VLAN has no sub-VLANs by default.

The VLANs to be configured as the sub-VLANs of the IPv6 multicast VLAN must exist and must not be IPv6 multicast VLANs or sub-VLANs of any other IPv6 multicast VLAN.

The number of sub-VLANs of the IPv6 multicast VLAN must not exceed the system-defined limit.

Examples

```
# Configure VLAN 10 through VLAN 15 as sub-VLANs of IPv6 multicast VLAN 100.
```

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

```
[Sysname] multicast-vlan ipv6 100
```

```
[Sysname-ipv6-mvlan-100] subvlan 10 to 15
```

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

<http://www.hp.com/support>

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

<http://www.hp.com/go/wwalerts>

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

<http://www.hp.com/support/manuals>

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Websites

- HP.com <http://www.hp.com>
- HP Networking <http://www.hp.com/go/networking>
- HP manuals <http://www.hp.com/support/manuals>
- HP download drivers and software <http://www.hp.com/support/downloads>
- HP software depot <http://www.software.hp.com>
- HP Education <http://www.hp.com/learn>

Conventions

This section describes the conventions used in this documentation set.





Command conventions

Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> 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 bold text. For example, the New User window appears; 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

	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 switching engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a security product, such as a firewall, a UTM, or a load-balancing or security card that is installed in a device.
	Represents a security card, such as a firewall card, a load-balancing card, or a NetStream card.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index

D E G H I L M O P R S

D

display igmp-snooping group, 1
display igmp-snooping host, 2
display igmp-snooping statistics, 4
display mac-address multicast, 5
display mld-snooping group, 46
display mld-snooping host, 47
display mld-snooping statistics, 49
display multicast-vlan, 42
display multicast-vlan ipv6, 85
display pim-snooping ipv6 neighbor, 80
display pim-snooping ipv6 routing-table, 81
display pim-snooping ipv6 statistics, 82
display pim-snooping neighbor, 37
display pim-snooping routing-table, 38
display pim-snooping statistics, 39
dot1p-priority (IGMP-snooping view), 6
dot1p-priority (MLD-snooping view), 50
dscp (IGMP-snooping view), 7
dscp (MLD-snooping view), 50

F

fast-leave (IGMP-snooping view), 7
fast-leave (MLD-snooping view), 51

G

group-policy (IGMP-snooping view), 8
group-policy (MLD-snooping view), 52

H

host-aging-time (IGMP-snooping view), 9
host-aging-time (MLD-snooping view), 53
host-tracking (IGMP-snooping view), 10
host-tracking (MLD-snooping view), 53

I

igmp-snooping, 10
igmp-snooping access-policy, 11
igmp-snooping dot1p-priority, 12
igmp-snooping drop-unknown, 12

igmp-snooping enable, 13
igmp-snooping fast-leave, 14
igmp-snooping general-query source-ip, 14
igmp-snooping group-limit, 15
igmp-snooping group-policy, 16
igmp-snooping host-aging-time, 17
igmp-snooping host-join, 18
igmp-snooping host-tracking, 19
igmp-snooping last-member-query-interval, 19
igmp-snooping leave source-ip, 20
igmp-snooping max-response-time, 21
igmp-snooping overflow-replace, 22
igmp-snooping proxying enable, 23
igmp-snooping querier, 23
igmp-snooping query-interval, 24
igmp-snooping report source-ip, 25
igmp-snooping router-aging-time, 25
igmp-snooping router-port-deny, 26
igmp-snooping source-deny, 27
igmp-snooping special-query source-ip, 27
igmp-snooping static-group, 28
igmp-snooping static-router-port, 29
igmp-snooping version, 30

L

last-listener-query-interval (MLD-snooping view), 54
last-member-query-interval (IGMP-snooping view), 31

M

mac-address multicast, 31
max-response-time (IGMP-snooping view), 32
max-response-time (MLD-snooping view), 54
mld-snooping, 55
mld-snooping access-policy, 56
mld-snooping done source-ip, 56
mld-snooping dot1p-priority, 57
mld-snooping drop-unknown, 58
mld-snooping enable, 59
mld-snooping fast-leave, 59

- mld-snooping general-query source-ip, [60](#)
- mld-snooping group-limit, [61](#)
- mld-snooping group-policy, [62](#)
- mld-snooping host-aging-time, [63](#)
- mld-snooping host-join, [64](#)
- mld-snooping host-tracking, [65](#)
- mld-snooping last-listener-query-interval, [65](#)
- mld-snooping max-response-time, [66](#)
- mld-snooping overflow-replace, [67](#)
- mld-snooping proxying enable, [67](#)
- mld-snooping querier, [68](#)
- mld-snooping query-interval, [69](#)
- mld-snooping report source-ip, [69](#)
- mld-snooping router-aging-time, [70](#)
- mld-snooping router-port-deny, [71](#)
- mld-snooping source-deny, [72](#)
- mld-snooping special-query source-ip, [72](#)
- mld-snooping static-group, [73](#)
- mld-snooping static-router-port, [74](#)
- mld-snooping version, [75](#)
- multicast-vlan, [43](#)
- multicast-vlan ipv6, [86](#)

O

- overflow-replace (IGMP-snooping view), [33](#)
- overflow-replace (MLD-snooping view), [75](#)

P

- pim-snooping enable, [40](#)
- pim-snooping ipv6 enable, [83](#)
- port (IPv6 multicast VLAN view), [87](#)
- port (multicast VLAN view), [44](#)
- port multicast-vlan, [44](#)
- port multicast-vlan ipv6, [87](#)

R

- report-aggregation (IGMP-snooping view), [34](#)
- report-aggregation (MLD-snooping view), [76](#)
- reset igmp-snooping group, [34](#)
- reset igmp-snooping statistics, [35](#)
- reset mld-snooping group, [77](#)
- reset mld-snooping statistics, [77](#)
- reset pim-snooping ipv6 statistics, [84](#)
- reset pim-snooping statistics, [41](#)
- router-aging-time (IGMP-snooping view), [35](#)
- router-aging-time (MLD-snooping view), [78](#)

S

- source-deny (IGMP-snooping view), [36](#)
- source-deny (MLD-snooping view), [78](#)
- subvlan (IPv6 multicast VLAN view), [88](#)
- subvlan (multicast VLAN view), [45](#)